



Ghidul de acasă pentru Siguranță Digitală



Securitate digitală

Pentru familii cu copii între 5 și 12 ani
Un sprijin practic pentru conversații mai simple, reguli mai
clare și mai multă liniște în relația copilului cu tehnologia.

RoboticsSchool.ro



ROBOTICS



SCHOOL

Bun venit

Dacă ai deschis acest ghid, probabil simți deja un lucru foarte simplu: tehnologia este deja parte din viața copilului tău.

Nu mai vorbim doar despre desene animate sau câteva minute pe tabletă. Vorbim despre jocuri, chat, video-uri, reclame, linkuri, aplicații, mesaje și, uneori, despre situații care apar mai repede decât ai fi crezut.

Vestea bună este că nu ai nevoie să fii expert în tehnologie ca să creezi mai multă siguranță acasă.

Ai nevoie de:

câteva setări bune,

reguli simple,

reacții clare când apare o problemă,

și un limbaj pe care copilul îl poate înțelege.

Acest ghid este făcut exact pentru asta.

Nu ca să te sperie.

Nu ca să complice lucrurile.

Ci ca să te ajute să înțelegi ce contează, ce merită setat și cum poți preveni cele mai frecvente probleme.



RoboticsSchool.ro



ROBOTICS



SCHOOL

Ce înseamnă, concret, siguranță digitală

Siguranța digitală nu înseamnă doar „să nu vorbească cu străini”.

În practică, înseamnă să reduci câteva riscuri foarte reale:

- copilul să nu dea informații personale;
- copilul să nu intre în conversații nepotrivite;
- copilul să nu apese pe linkuri, reclame sau ferestre suspecte;
- copilul să nu poată cumpăra, instala sau activa lucruri fără să știi;
- copilul să știe ce face dacă vede ceva care îl sperie sau îl încurcă;
- tu să ai vizibilitate asupra aplicațiilor, conturilor și setărilor importante.

Pe scurt, siguranța digitală înseamnă două lucruri: prevenție și reacție bună.

Prevenție: setezi și explici câteva lucruri înainte.

Reacție bună: știi ce faci dacă apare o problemă.



RoboticsSchool.ro



ROBOTICS



SCHOOL

1. Ce merită setat pe telefon, tabletă sau laptop

Aici este una dintre cele mai utile părți ale ghidului.

Nu ai nevoie de cunoștințe tehnice avansate. Dar sunt câteva lucruri care merită făcute de la început.

Ce să verifici pe dispozitiv

1. Pune un cod de acces pe dispozitiv

Telefonul, tableta sau laptopul ar trebui să aibă cod, parolă sau autentificare biometrică.

Asta nu este doar pentru securitate generală, ci și pentru a evita accesul necontrolat la setări, cumpărături sau instalări.

2. Activează actualizările automate

Actualizările nu aduc doar funcții noi. Ele repară și vulnerabilități de securitate.

Verifică:

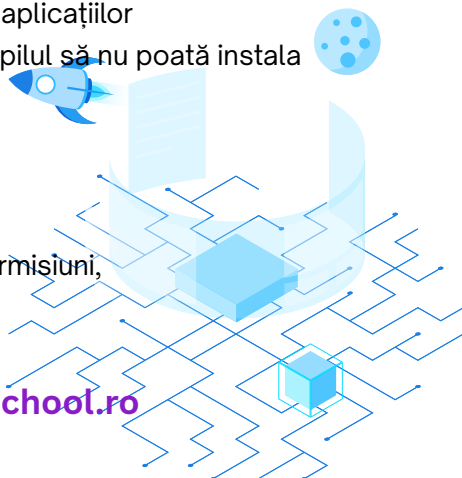
- sistemul de operare,
- browserul,
- aplicațiile folosite des.

3. Cere aprobare pentru instalarea aplicațiilor

Setează dispozitivul astfel încât copilul să nu poată instala aplicații singur.

Asta te ajută să eviți:

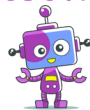
- aplicații nepotrivite,
- jocuri cu reclame agresive,
- aplicații care cer prea multe permisiuni,
- instalări făcute din curiozitate.



RoboticsSchool.ro



ROBOTICS



SCHOOL

4. Verifică permisiunile aplicațiilor

Intră în setările dispozitivului

și uită-te la ce aplicații au acces la:

- cameră/ microfon,
- locație / fotografii,
- contacte.

Dacă o aplicație nu are nevoie reală de o permisiune, oprește-o.

5. Oprește sau protejează cumpărăturile din aplicații

Unele jocuri și aplicații sunt făcute să încurajeze apăsarea rapidă: „cumpără”, „deblochează”, „continuă”, „ia acum”.

Verifică să existe:

- parolă pentru fiecare achiziție,
- blocarea cumpărăturilor, unde se poate,
- notificări pentru plăți.

6. Folosește cont de copil sau control parental unde există

Pe multe dispozitive și platforme există versiuni de cont pentru copii sau opțiuni de control parental.

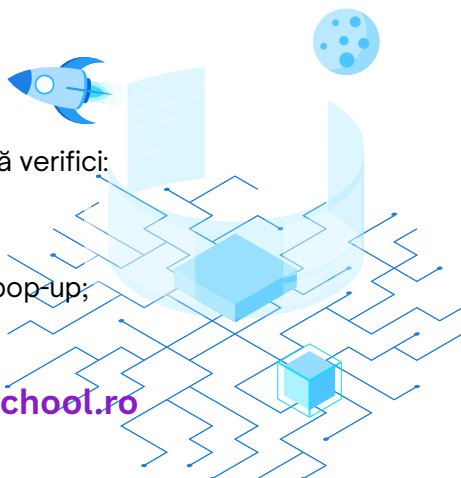
Acestea te ajută să:

- limitezi descărcările,
- vezi timpul de utilizare,
- filtrezi conținutul,
- controlezi anumite funcții.

7. Verifică browserul

Dacă folosește browserul, e bine să verifici:

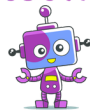
- ce motor de căutare este setat;
- dacă există filtre de conținut;
- dacă se pot deschide ferestre pop-up;
- dacă istoricul poate fi verificat.



RoboticsSchool.ro



ROBOTICS



SCHOOL

2. Ce informații nu se dau niciodată online

Aici merită să fii foarte clar. Nu cu explicații lungi, ci cu o regulă simplă.

Copilul tău nu oferă online, în jocuri, în chat sau în aplicații:

- numele complet;
- adresa;
- numărul de telefon;
- numele școlii;
- parola;
- coduri primite prin SMS sau email;
- locația;
- poze sau video trimise la cerere;
- programul zilnic;
- informații despre unde este acum sau unde merge.

Mesajul simplu pentru copil

Numele complet, adresa, școala, parola, codurile și pozele nu se dau online fără tine.

Este bine ca această regulă să fie repetată clar și scurt.

Nu presupune că „sigur știe deja”.



RoboticsSchool.ro



ROBOTICS



SCHOOL

3. Ce riscuri apar cel mai des la copiii de 5–12 ani

Când spui „siguranță digitală”, multe riscuri par abstracte. În realitate, cele mai frecvente situații sunt foarte concrete.

Cele mai comune riscuri sunt:

1. Reclame care par butoane normale

Multe jocuri și site-uri afișează reclame care seamănă cu:

- buton de Play, Next,
- Continue,
- Reward,
- Close.

Copilul poate apăsa fără să realizeze că nu face parte din joc.

2. Linkuri sau ferestre care promit ceva

De tipul:

- „Ai câștigat!”
- „Deschide acum!”
- „Primești monede gratuite!”
- „Apasă aici ca să continui!”

Acestea pot duce spre site-uri nepotrivite, descărcări sau cereri de date.

3. Mesaje de la necunoscuți

În jocuri, pe rețele sociale sau pe platforme cu chat, cineva necunoscut poate începe o conversație aparent banală:

- „Salut” „Câți ani ai?”
- „De unde ești?”
- „Jucăm împreună?”
- „Hai pe altă aplicație”





ROBOTICS



SCHOOL

4. Presiune să păstreze un secret

Asta este una dintre cele mai importante alerte.

Dacă cineva îi spune:

- „nu le spune părinților”,
- „e doar între noi”,
- „dacă spui, nu mai vorbim”,

este deja o situație care cere oprire și anunțarea ta.

5. Cumpărături accidentale sau apăsări rapide

Copiii pot confirma o achiziție fără să înțeleagă ce fac, mai ales dacă jocul îi presează cu viteză.

6. Conținut care pornește de la ceva „ok” și duce spre altceva

Un video poate părea potrivit la început și apoi, prin recomandări, să ducă spre alt conținut:

- mai agresiv,
- mai nepotrivit,
- mai captivant decât ai vrea.





ROBOTICS



SCHOOL

4. Cum îi explici copilului regulile, simplu

Nu este nevoie de un discurs lung. Este mai util să ai câteva propoziții clare, pe care să le repeți.

Mesaje utile

- „Dacă apare ceva nou sau ciudat, nu apeși singur.”
- „Dacă cineva îți scrie și nu îl cunoști, îmi arăți.”
- „Nu dăm numele complet, adresa, școala sau parola.”
- „Dacă te sperie ceva, vii la mine imediat.”
- „Dacă cineva îți cere să păstrezi secretul, îmi spui.”
- „Dacă nu ești sigur, te oprești și mă chemi.”

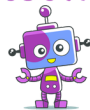
Aceste propoziții funcționează pentru că sunt:

- scurte,
- clare,
- ușor de ținut minte.





ROBOTICS



SCHOOL

4. Cum îi explici copilului regulile, simplu

Nu este nevoie de un discurs lung. Este mai util să ai câteva propoziții clare, pe care să le repeți.

Mesaje utile

- „Dacă apare ceva nou sau ciudat, nu apeși singur.”
- „Dacă cineva îți scrie și nu îl cunoști, îmi arăți.”
- „Nu dăm numele complet, adresa, școala sau parola.”
- „Dacă te sperie ceva, vii la mine imediat.”
- „Dacă cineva îți cere să păstrezi secretul, îmi spui.”
- „Dacă nu ești sigur, te oprești și mă chemi.”

Aceste propoziții funcționează pentru că sunt:

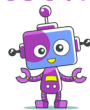
- scurte,
- clare,
- ușor de ținut minte.



RoboticsSchool.ro



ROBOTICS



SCHOOL

5. Cum procedezi când copilul este logat în jocuri cu chat

Aici apar multe riscuri pe care părinții le subestimează, pentru că jocul pare „doar un joc”.

Dar dacă jocul are:

- chat public,
- mesaje private,
- cereri de prietenie,
- posibilitatea de a trimite linkuri,
- voce sau comentarii live,

atunci jocul nu mai este doar joc. Are și componentă socială.

Ce merită verificat înainte

- există chat public?
- există mesaje private?
- poate primi cereri de prietenie?
- poate trimite sau primi linkuri?
- există cumpărături în joc?
- poate activa microfonul?

Ce e util să setezi

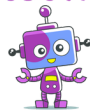
- oprește chatul dacă nu este necesar;
- limitează cine poate trimite mesaje;
- dezactivează microfonul dacă jocul nu are nevoie de el;
- protejează cumpărăturile;
- verifică dacă jocul permite blocare și raportare.

RoboticsSchool.ro





ROBOTICS



SCHOOL

Ce reguli simple îți spui copilului

- nu răspunzi la mesaje de la necunoscuți;
- nu spui câți ani ai, unde locuiești sau la ce școală mergi;
- nu accepți să muți conversația pe altă aplicație;
- nu trimiți poze, audio sau video;
- dacă cineva insistă sau întreabă prea mult, îți arăți imediat.

Semne că o conversație nu este ok

- te întreabă unde stai;
- te întreabă dacă ești singur;
- îți cere poză;
- îți cere cont de altă aplicație;
- îți spune să nu spui părinților;
- te grăbește să răspunzi;
- încearcă să fie „prea apropiat” prea repede.

Ce faci dacă apare o situație de genul acesta

- oprești conversația;
- faci captură de ecran, dacă poți;
- blochezi utilizatorul;
- raportezi contul în joc;
- verifici dacă a trimis și altceva;
- schimbi parola dacă este nevoie.

Regula-cheie:

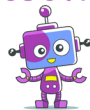
În jocurile cu chat, faptul că este „un alt jucător” nu înseamnă că este sigur.



RoboticsSchool.ro



ROBOTICS



SCHOOL

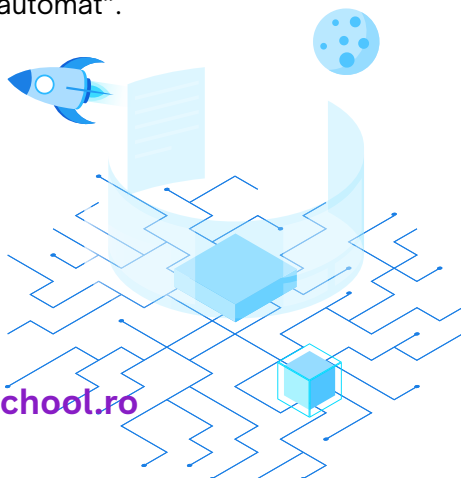
6. Cum procedezi cu rețelele sociale

Pentru copiii între 5 și 12 ani, problema nu este doar dacă au sau nu cont. Problema este că pot ajunge foarte ușor la conținut de pe rețele sociale:

- prin frați mai mari,
- prin colegi,
- prin clipuri distribuite,
- prin conturi făcute prea devreme,
- prin Shorts, Reels sau alte formate scurte.

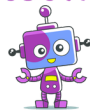
Ce riscuri apar aici

- conturi publice;
- cereri de prietenie de la necunoscuți;
- mesaje directe;
- presiune să posteze;
- distribuirea de poze sau video;
- expunerea locației sau a rutinei;
- conținut nepotrivit care apare „automat”.





ROBOTICS



SCHOOL

Dacă există acces la o rețea socială, regulile minime sunt:

- contul trebuie să fie privat;
- parola este cunoscută de tine;
- nu acceptă persoane necunoscute;
- nu postează numele complet, școala, adresa, programul sau locația;
- nu trimite poze sau video la cerere;
- nu răspunde la mesaje de la necunoscuți;
- nu mută conversațiile pe alte aplicații.
-

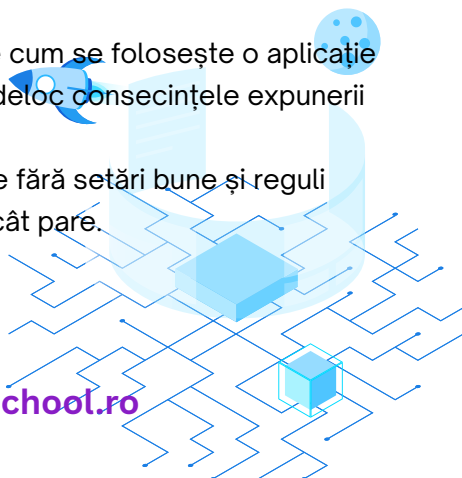
Ce merită verificat în setări

- profil privat, nu public;
- cine poate trimite mesaje;
- cine poate comenta;
- cine poate vedea lista de prieteni sau urmăritori;
- dacă locația este oprită;
- dacă aplicația poate accesa contactele.

Ce merită să ții minte

Un copil poate înțelege foarte bine cum se folosește o aplicație și, în același timp, să nu înțeleagă deloc consecințele expunerii online.

De aceea, accesul la rețele sociale fără setări bune și reguli clare creează mai multe riscuri decât pare.





ROBOTICS



SCHOOL

7. Ce faci când alt copil îți arată ceva pe telefon sau îți trimite ceva

Aici apar multe situații pe care părinții nu le anticipează.
Nu tot ce ajunge la copil vine dintr-o aplicație instalată de tine.
Poate veni:

- de la un coleg;
- de la un verișor;
- de pe telefonul altui copil;
- printr-un link primit;
- printr-un joc în care cineva distribuie ceva.

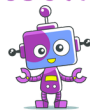
Ce poate primi

- clipuri nepotrivite;
- provocări sau „challenge-uri”;
- linkuri;
- glume agresive;
- conținut care îl sperie;
- mesaje de tip „uită-te repede și să nu spui”.
-





ROBOTICS



SCHOOL

Mesajul important pentru copil

Faptul că vine de la un alt copil nu înseamnă automat că este sigur.

Ce îi poți spune simplu

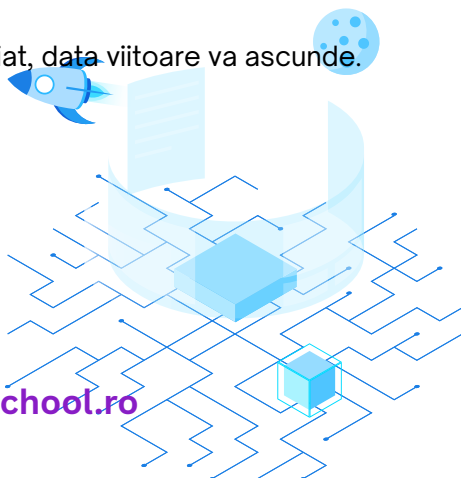
- „Dacă cineva îți arată ceva care te sperie sau te încurcă, îmi spui.”
- „Dacă primești un link, nu îl deschizi singur.”
- „Dacă cineva spune «să nu le spui părinților», exact atunci îmi spui.”

Ce faci dacă s-a întâmplat deja

- afli calm ce a văzut sau ce a primit;
- nu îl faci să se simtă vinovat pentru că ți-a spus;
- verifici dispozitivul sau mesajul;
- blochezi sau ștergi ce trebuie;
- repeți regula simplă pentru data viitoare.

Aici contează mult reacția ta.

Dacă se teme că va fi certat imediat, data viitoare va ascunde.





ROBOTICS



SCHOOL

8. Semne că ceva nu este în regulă

Nu toate problemele digitale se văd imediat pe ecran. Uneori se văd mai întâi în comportament.

Semne la care merită să fii atent

- închide rapid ecranul când te apropii;
- devine tensionat după ce stă online;
- se sperie sau se irită neobișnuit de tare;
- insistă brusc pentru mai multă intimitate digitală;
- primește mesaje și evită să spună de la cine;
- pare rușinat sau neliniștit după un joc sau o aplicație;
- vorbește despre „secrete” legate de cineva cunoscut online;
- cere să instaleze o aplicație „pentru că o au și ceilalți”, dar evită să explice ce face.

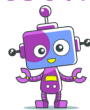
Niciun semn singur nu dovedește ceva grav. Dar mai multe semne împreună merită verificate.



RoboticsSchool.ro



ROBOTICS



SCHOOL

9. Ce faci dacă apare o problemă

Când apare ceva neplăcut, ajută mult să ai o ordine clară.

Pasul 1: oprești situația

Închizi aplicația, jocul, conversația sau pagina respectivă

Pasul 2: verifici ce s-a întâmplat

Află concret:

- ce a apărut, cine a scris;
- pe ce platformă, dacă a apăsat pe ceva;
- dacă a trimis ceva,
- dacă a apărut o plată sau o instalare.

Pasul 3: păstrezi dovezi dacă e nevoie

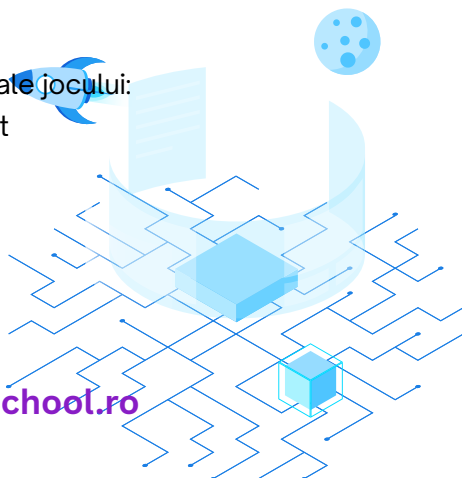
Dacă este o conversație, o amenințare, o cerere suspectă sau un comportament repetat:

- fă o captură de ecran;
- notează numele contului sau al jocului.

Pasul 4: blochezi și raportezi

Folosește funcțiile platformei sau ale jocului:

- Block / Report / Mute / Restrict





Pasul 5: verifici contul

Dacă a apăsăat pe linkuri sau a introdus date:

- schimbă parola;
- verifică emailul asociat;
- verifică dacă au fost instalate aplicații noi;
- verifică dacă au existat plăți sau aprobări.

Pasul 6: explici simplu, fără panică

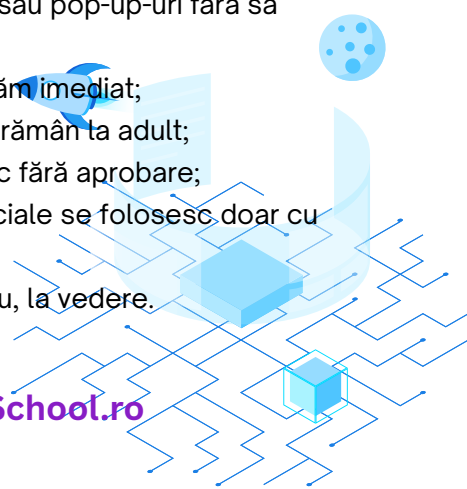
Este nevoie de claritate:

- ce s-a întâmplat /de ce nu este ok;
- ce va face data viitoare.

10. Reguli simple de siguranță digitală pentru familie

- Aici funcționează mai bine puține reguli, dar clare.
- Un set bun de reguli poate fi:
- nu instalăm aplicații fără acord;
- nu răspundem la mesaje de la necunoscuți;
- nu dăm date personale;
- nu apăsăm pe linkuri, reclame sau pop-up-uri fără să verificăm;
- dacă apare ceva ciudat, anunțăm imediat;
- parolele și setările importante rămân la adult;
- cumpărăturile digitale nu se fac fără aprobare;
- jocurile cu chat și conturile sociale se folosesc doar cu setările potrivite.

Aceste reguli pot fi și scrise simplu, la vedere.





11. Checklist de siguranță digitală

Poți folosi lista de mai jos ca verificare rapidă.

Dispozitiv

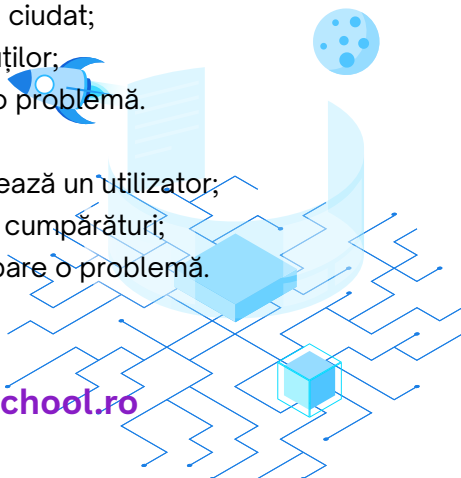
- are cod de acces;
- are actualizările pornite;
- aplicațiile nu se instalează fără aprobare;
- cumpărăturile sunt blocate sau protejate;
- permisiunile pentru cameră, microfon și locație au fost verificate.

Conturi și aplicații

- știi ce aplicații folosește;
- știi ce conturi există;
- știi parolele importante;
- știi dacă există chat, mesaje private sau cumpărături în jocuri;
- profilurile sociale, dacă există, sunt private.

Reguli

- copilul știe ce informații nu se dau online;
- știe ce să facă dacă vede ceva ciudat;
- știe că nu răspunde necunoscuților;
- știe că vine la tine dacă apare o problemă.
- Situații speciale
- știi cum se blochează și raportează un utilizator;
- știi cum verifici dacă s-au făcut cumpărături;
- știi cum schimbi parola dacă apare o problemă.





ROBOTICS



SCHOOL

Încheiere

Siguranța digitală nu stă într-o singură aplicație și nici într-o singură discuție.

Ea se construiește din lucruri concrete:

- setări bune și reguli clare;
- reacții calme;
- și câteva reflexe simple pe care copilul le poate învăța.

Nu trebuie să știi tot.

Dar ajută mult să știi ce contează.

Iar când regulile sunt clare și pașii sunt simpli, relația copilului cu tehnologia devine mai sigură și mai ușor de gestionat.

Dacă simți că în familia ta e nevoie de mai multă claritate și sprijin pe partea de siguranță digitală, am creat programul de workshop-uri **Digital Hero**.

Un program practic, dedicat copiilor, în care învață pe înțelesul lor cum să recunoască riscurile din online, cum să reacționeze în situații neclare și cum să folosească tehnologia cu mai multă atenție și responsabilitate.

Pentru a verifica calendarul de workuri, ne poți scrie direct la +40 724 124 868

Cu drag, Echipa Robotics School
Stai în siguranță!



RoboticsSchool.ro