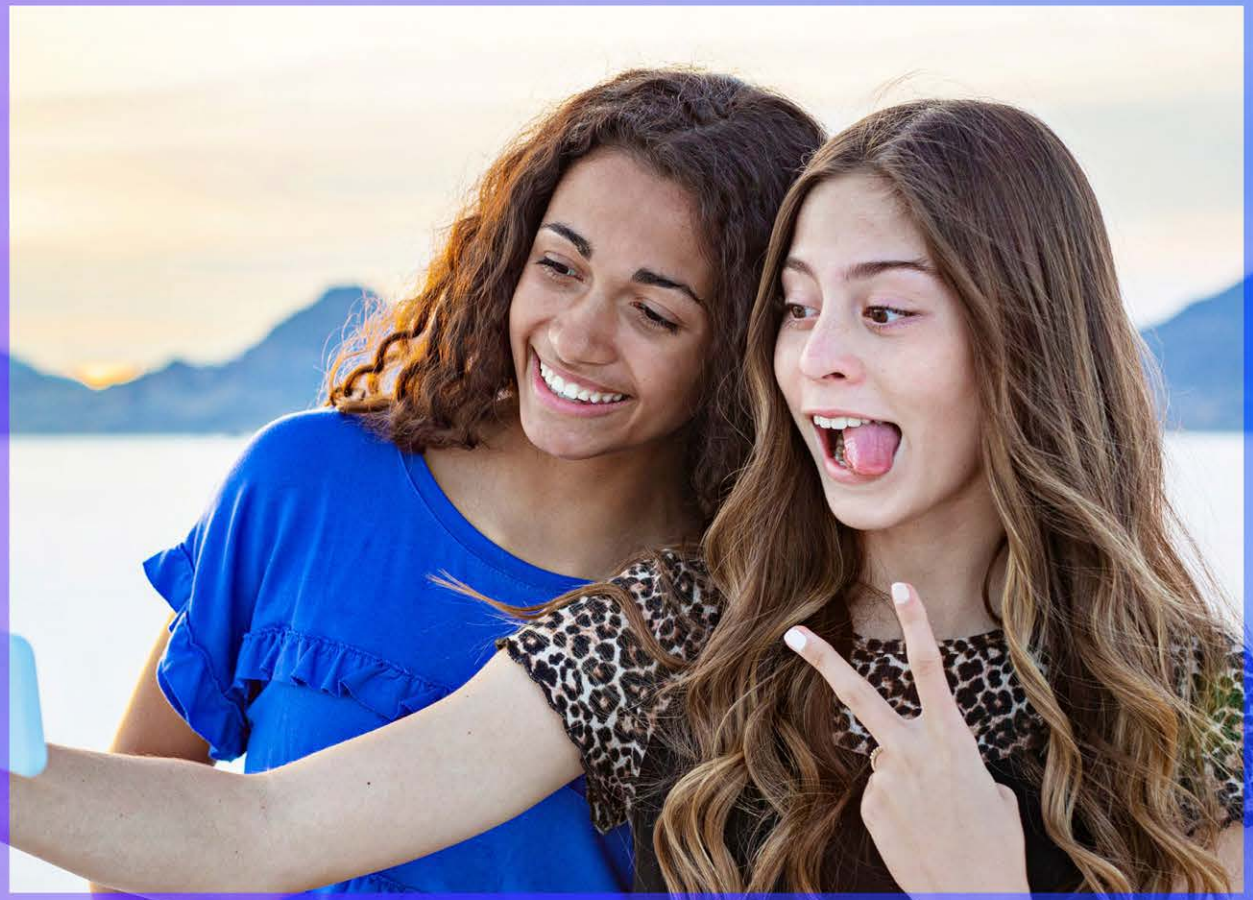
# Fii inteligent în mediul cibernetic!



**Cum să păstrăm copiii în siguranță online - un ghid pentru părinți.**

KPMG în România | kpmg.com/cyberday

Internetul este un instrument puternic care le oferă copiilor oportunități nelimitate de a învăța, de a socializa și de a se distra. Cu toate acestea, având în vedere că o treime din utilizatorii de internet au sub 18 ani, riscurile online au devenit o preocupare semnificativă și continuă să crească. Anul trecut, aproape trei din patru copii din întreaga lume s-au confruntat cu cel puțin un risc cibernetic. De aceea, este esențial să începeți să discutați despre siguranța pe internet cu copiii dumneavoastră de la o vârstă fragedă. În acest fel, îi puteți ajuta să facă alegeri în cunoștință de cauză și să dezvolte obiceiuri online sănătoase. Educându-i cu privire la utilizarea responsabilă a internetului, la protecția vieții private și la pericolele potențiale, îi veți ține, de asemenea, la adăpost de riscuri. Nu uitați, niciodată nu este prea devreme pentru a pune bazele unei utilizări sigure a internetului. Pentru a vă ajuta să vă păstrați copiii în siguranță, explorați ghidul pentru părinți *Fii inteligent în mediul cibernetic!* privind siguranța pe internet, care oferă sfaturi valoroase. În calitate de părinte sau tutore, protejarea bunăstării online a copilului dumneavoastră este mai importantă ca niciodată.



# Vorbiți din timp despre siguranța în mediul online și fiți un părinte proactiv

Începeți să vorbiți cu copiii dumneavoastră de la o vârstă fragedă despre siguranța pe Internet. Prin intermediul acestor discuții timpurii, îi puteți ajuta să facă alegeri inteligente și să dezvolte obiceiuri online sănătoase. Educarea copiilor cu privire la utilizarea responsabilă a Internetului, la protecția vieții private și la pericolele potențiale îi va proteja de riscurile ce pot surveni. Nu uitați, niciodată nu este prea devreme pentru a pune bazele unei utilizări sigure a Internetului.

- **Tinerii sunt întotdeauna dornici să învețe.** Educați-i în privința folosirii parolelor sigure, identificării paginilor web securizate, recunoașterii înșelăciunilor, a comportamentului online adecvat și altor abilități pentru o activitate online sigură.
- **Nu furniza informații personale.** Amintiți-le copiilor să nu furnizeze niciodată informații personale, cum ar fi numele complet, adresa locuinței, parolele sau numerele de telefon, către orice persoană necunoscută.
- **Fii atent cu străinii.** Discutați cu copiii dumneavoastră despre potențialele pericole ale interacțiunii cu persoane străine online și avertizați-i să nu se întâlnească vreodată cu cineva în persoană fără știrea și acordul dvs.
- **Puneți întrebări.** Asigurați-vă că îl întrebați pe copilul dvs. despre ceea ce face online, cum ar fi ce pagini de Internet vizitează și cu cine vorbește. Încurajați-l să fie deschis în privința a ceea ce spune și vede în timp ce este online.
- **Stabiliți reguli clare și precise.** Controlați timpul petrecut în fața ecranului stabilind limite pentru cât timp copilul dvs. stă online și ce activități poate desfășura. Timpul petrecut în fața ecranului, care nu este legat de teme școlare, poate fi disponibil după terminarea temelor sau la sfârșitul săptămânii. Păstrați calculatoarele și dispozitivele într-o zonă comună pentru a supraveghea toate activitățile.
- **Restricționați accesul la Internet și monitorizați activitatea.** Nu trebuie să fiți expert în cibernetică pentru a vă proteja copiii online. Aplicațiile de control parental și cele integrate în dispozitive și echipamente de tip router Wi-Fi sunt ușor de utilizat. Aceste controale vă permit să stabiliți perioade de acces, să monitorizați activitatea pe Internet și să blocați anumite categorii de pagini pe Internet. Știind ce fac copiii dvs. online puteți contribui la siguranța lor. Folosiți această ocazie pentru a le arăta copiilor dvs. care sunt paginile de Internet potrivite pentru grupa lor de vârstă.
- **Puneți în practică ceea ce îl învățați.** Oferiți un bun exemplu cu propria dvs. prezență online. Demonstrați un comportament și practici sigure.

# Jocuri online? Joacă inteligent!

În timp ce jocurile online pot oferi ore de distracție și interacțiune socială, există și o latură mai întunecată. De la ”hărțuire cibernetică” (cyberbulling) la prădători online și costuri ascunse, există multe preocupări atunci când vine vorba de jocurile video online, în special pentru copii. Iată cum vă puteți proteja copiii:

- Implementați restricțiile disponibile pentru a-i împiedica să descarce aplicații necorespunzătoare.
- Configurați parole pentru a preveni achizițiile în joc.
- Stabiliți așteptări clare și reguli pentru limitele de timp și jocurile permise.
- Limitați conversațiile în chat la cele relevante pentru joc.
- Asigurați-vă că copilul dvs. înțelege ce înseamnă informațiile personale și că nu ar trebui să le împărtășească niciodată online.
- Spuneți-le să raporteze orice hărțuire sau comportament agresiv unui adult imediat.



# Sfaturi de siguranță pentru rețelele sociale

Platformele rețelelor de socializare au devenit parte integrantă din viața noastră de zi cu zi și valoroase instrumente pentru comunicare și divertisment. Cu toate acestea, există și riscuri semnificative asociate acestor platforme, în special pentru copii. Utilizarea abuzivă a rețelelor de socializare de către copii îi poate expune pe aceștia la diverse pericole, inclusiv cyberbulling și la prădătorii online.

Pentru a vă păstra copiii în siguranță, iată câteva sfaturi de care trebuie să țineți cont:

- **Restricții de vârstă.** Majoritatea platformelor de socializare au restricții de vârstă. Asigurați-vă că acestea sunt respectate și monitorizați utilizarea lor.
- **Faceți o pauză înainte de a posta.** Învățați-vă copiii să fie atenți la comentariile și fotografiile pe care le postează și subliniați să nu împărtășească niciodată informații personale precum vârsta, școala, adresa sau numele complet. Explicați-le că odată ce sunt online, informațiile rămân permanent pe Internet. Acest lucru este deosebit de important pe măsură ce copiii cresc și caută locuri de muncă de vară - majoritatea angajatorilor vor face o verificare generală a potențialilor candidați.
- **Urmăriți-vă copilul.** Monitorizați activitatea de pe rețelele de socializare urmărindu-vă copilul online. Nu trebuie să participați, ci doar să vizualizați profilurile și postările în mod regulat.
- **Revizuiți paginile de îndrumare parentală din social media.** Pentru a afla mai multe despre protecția copiilor dvs. pe rețelele de socializare, consultați paginile de îndrumare pentru părinți. Asigurați-vă că profilul copilului dvs. este întotdeauna activat pe modul "privat" prin intermediul configurațiilor contului și învățați-i despre importanța activării setărilor de confidențialitate ale rețelelor de socializare.

# Cyberbullying

Agresiunea în mediul online (cyberbullying) este o formă de hărțuire/ agresiune utilizând forme electronice de contact și din păcate a devenit tot mai frecventă. Deși similară cu agresiunea din tip bullying obișnuită, cea de tip cyberbullying duce trauma un pas mai departe, permițând agresorilor să urmărească victima oriunde merge. Practic oricine, oriunde, oricând poate hărțui o altă persoană, doar conectându-se la Internet sau utilizând un telefon mobil. Iată cum puteți ajuta:

## Comunicare

Este crucial astăzi să vorbim deschis cu copiii despre cyberbullying. Educați-i să:

- Raporteze imediat comentariile ofensatoare sau jignitoare, indiferent dacă sunt ținta lor sau nu.
- Aibă grijă la ceea ce spun, trimit, postează sau scriu despre alții — hărțuirea neintenționată este tot hărțuire.

## Recunoaștere

Semne ale faptului că cineva este victimă a fenomenului cyberbullying:

- Manifestarea unei furii, depresii sau frustrări neașteptate după folosirea unui dispozitiv sau evitarea utilizării dispozitivului în întregime.
- Nesiguranța sau anxietatea referitoare la mersul la școală sau participarea la activități de grup sau de echipă.
- Retragerea anormală din activitățile cu prietenii și/sau membrii ai familiei.

## Acțiune

Este important ca părinții și copiii să acționeze prin:

- Salvarea mesajelor, postărilor și mesajelor email de hărțuire.
- A nu răspunde și a nu le șterge.
- Raportarea contului agresor online și blocarea acestuia de la interacțiuni ulterioare.
- Escaladarea problemei la școala copilului sau la poliție, după caz.

# Conectarea și deconectarea în siguranță

Păstrarea evidenței parolelor poate fi o problemă, îndeosebi pentru copiii care au probleme a și le aminti pe toate. Cu toate acestea, este important să recunoaștem că parolele reprezintă principala măsură de protecție împotriva posibilelor încălcări ale confidențialității care pot afecta siguranța atât online, cât și offline. Pentru a asigura procese sigure de conectare și deconectare, iată câteva sfaturi cheie pentru a-i ajuta pe copiii dvs. să își protejeze mai bine datele personale.

**Alegeți cu grijă numele de utilizator**

- Evitați utilizarea numelui complet, vârstei, adresei, datei de naștere, genului sau a altor informații personale.
- Sfătuiți copiii să ceară sfatul unui adult în caz de îndoială cu privire la alegerea numelui de utilizator.

**Practicați siguranța parolelor**

- Arătați-le copiilor cum să combine expresii, numere, simboluri și litere mari și mici.
- Subliniați să nu repete sau să refolosească parolele și să nu le împărtășească niciodată sau să le furnizeze la cerere.
- Evitați parolele ușor de ghicit, precum data nașterii sau sportul sau activitatea preferată.
- Încercați să utilizați un manager de parole și sugerați copiilor să-și amintească doar trei parole: una pentru școală, una pentru computerul lor și una pentru managerul de parole — cu toate celelalte parole stocate acolo.
- Încurajați-i să utilizeze autentificarea cu doi factori atunci când este posibil.

**Protejarea informațiilor personale**

- Reamintiți-i copilului dvs. să se deconecteze întotdeauna atunci când părăsește un site sau o platformă.
- Este cel mai bine să evitați rețelele Wi-Fi gratuite (pentru că există riscul furtului de date de către persoane rău intenționate/ hackeri).
- Nu partajați niciodată datele de autentificare cu alte persoane, nici măcar cu prietenii.
- Sfătuiți-vă copiii să nu ofere niciodată informații personale, cum ar fi numele complet, adresa de domiciliu sau numerele de telefon cuiva pe care nu le cunoaște.
- Când vizitați pagini de Internet de pe telefoane, nu introduceți nume de utilizator și parole.

# Cum folosim inteligența artificială în condiții de siguranță și securitate

Pe măsură ce programele de inteligență artificială (AI) câștigă popularitate, copiii vor deveni curioși în legătură cu acestea. Totuși, este esențial să purtăm discuții cu copiii despre utilizarea responsabilă și adecvată a tehnologiei. Luați în considerare următoarele sfaturi pentru a vă ajuta familia să exploreze și să învețe împreună despre AI:

**Cum funcționează?** Explicați-le copiilor dumneavoastră cum funcționează tehnologia AI, astfel încât aceștia să poată aprecia beneficiile sale, să înțeleagă potențialele sale limitări și să învețe cum să o folosească în mod eficient. Dați-le câteva exemple cu care ar putea fi deja familiarizați pentru a-i ajuta să înțeleagă despre ce este vorba.

**Cum să interacționezi?** Instrumentele de inteligență artificială îi pot ajuta pe copii să fie creativi și să dobândească noi abilități. Vorbiți cu copiii dvs. despre tehnologia AI. Faceți-i să se gândească la modul în care programele i-ar putea ajuta să învețe și să se dezvolte. Încurajați-i să fie critici față de informațiile pe care le obțin de la noile tehnologii AI și să își folosească creativitatea pentru a completa rezultatele primite de la acestea.

**Care sunt riscurile?** Copiii ar trebui să înțeleagă că inteligența artificială are limitări care pot cauza rezultate inexacte și distorsionate. De asemenea, hackerii pot manipula AI prin modificarea datelor, ceea ce poate duce la rezultate greșite. Nu uitați să le reamintiți copiilor că AI nu are o înțelegere emoțională și nu poate înlocui relațiile și conexiunile umane.

## Cum să folosiți AI în siguranță?

- **Fiți atenți la informațiile personale.** Copiii ar trebui să evite să împărtășească informații sensibile, precum numele lor complet, adresa, numărul de telefon sau informații financiare dacă nu au încredere în platformă și dacă nu cunosc modul în care aceasta gestionează datele cu caracter personal.
- **Înțelegeți setările de confidențialitate.** Acordați timp necesar pentru a revizui și a ajusta configurațiile de confidențialitate pe platformele de inteligență artificială în funcție de nivelul dumneavoastră de confort.
- **Nu exagerați cu împărtășirea de informații.** Limitați cantitatea de informații personale care sunt accesibile publicului și luați notă despre datele ce sunt colectate.
- **Gândiți în mod critic.** Nu uitați că sistemele de inteligență artificială nu sunt perfecte și pot face greșeli. Cereți-le copiilor să verifice informațiile, să verifice rezultatele din mai multe surse și să ia în considerare diferite perspective înainte de a ajunge la concluzii sau de a lua decizii bazate exclusiv pe rezultatele generate de inteligența artificială.
- **Raportați conținutul necorespunzător.** În cazul în care copilul dvs. întâlnește conținut ofensator sau periculos sau are parte de interacțiuni nepotrivite, instruiți-l să raporteze acest lucru platformei, furnizorului de servicii sau unui adult de încredere.
- **Fiți precauți cu mesajele generate de inteligența artificială.** Dacă primesc mesaje neașteptate sau suspecte de la conturi de AI sau de la roboți de coversație (**chatbots**), copiii nu trebuie să împărtășească informații personale și nu trebuie să se implice în discuții care îi fac să se simtă inconfortabil.
- **Nu vă bazați doar pe inteligența artificială.** Recomandați-le copiilor dvs. să nu se bazeze prea mult pe inteligența artificială pentru luarea deciziilor. Explicați copiilor că utilizarea AI pentru lucrări școlare ar putea fi considerată plagiat sau copiat. În schimb, introduceți instrumente educaționale de inteligență artificială care să le completeze învățarea.
- **Rămâneți informați.** Fiți la curent cu cele mai recente progrese și evoluții ale tehnologiei AI pentru a înțelege mai bine capacitățile, limitele și potențialul sistemelor AI riscuri potențiale. Aceste cunoștințe vor permite familiei dumneavoastră să facă alegeri în cunoștință de cauză și să utilizeze AI în mod responsabil.

# Șase moduri de a fi la curent cu securitatea cibernetică a copiilor dumneavoastră

## 01

**Fiți implicat în fiecare zi.**

Pentru a asigura siguranța copiilor dvs. online, rămâneți implicați și comunicați în mod frecvent cu aceștia. Înainte de a pune în aplicare orice măsuri de protecție, discutați cu copiii dumneavoastră despre motivele care stau la baza acestora, astfel încât aceștia să simtă că le respectați intimitatea.

## 02

**Controalele parentale.**

Luați în considerare utilizarea unei aplicații de control parental pentru a gestiona dispozitivele folosite de copiii dvs. și pentru a-i menține în siguranță online. Aceste aplicații vă pot ajuta prin blocarea conținutului web nedorit, restricționarea utilizării aplicațiilor riscante și multe altele. Este important să învățați cum să le folosiți și să le mențineți actualizate.

## 03

**Jurnalizarea și monitorizarea activității.**

Verificați periodic activitatea pe Internet a copilului dvs. cu ajutorul aplicației de control parental pentru a vă asigura că are practici și obiceiuri sigure. Discutați cu copiii dvs. despre paginile de Internet care sunt adecvate pentru grupa lor de vârstă și explicați-le de ce.

## 04

**Gestionați accesul la Internet.**

Supravegheați activitatea online a copilului dumneavoastră programând timpul petrecut pe Internet la ore prestabilite, cum ar fi după ce își termină temele sau la sfârșitul săptămânii (în weekend). Puteți utiliza aplicația de control parental pentru a limita timpul petrecut în fața ecranului.

## 05

**Instalarea soluțiilor de antivirus.**

Aceste programe reprezintă o linie de apărare puternică pentru a ajuta la protejarea computerelor și dispozitivelor de acasă împotriva virușilor și a altor tipuri de programe malware, care sunt din ce în ce mai frecvente. Subliniați importanța parolelor și a siguranței datelor personale.

## 06

**Efectuarea salvărilor de siguranță pentru dispozitiv (backup).**

Asigurați-vă că faceți o copie de rezervă a informațiilor importante pentru că datele se pierd. Pentru cei mai mulți, asta înseamnă păstrarea datelor originale pe dispozitivul utilizat, o copie de rezervă pe un hard disk extern și o alta în cloud.

## Informații și resurse suplimentare

Pentru a-i ajuta pe copii și adolescenți să dezvolte obiceiuri sigure pe Internet, părinții pot promova practici sigure și se pot implica. Pentru mai multe resurse despre obiceiurile de siguranță online, vizitați kpmg.com/cyberday.

### KPMG în România

#### București

Șoseaua București-Ploiești, nr. 89A,
Sector 1, București, 013685
**T:** +40 (372) 377 800
**F:** +40 (372) 377 700
**E:** kpmgro@kpmg.ro

www.kpmg.ro

#### Cluj-Napoca

Vivido Business Center
Strada Alexandru Vaida Voevod nr. 16,
Cluj-Napoca, 400592
**T:** +40 (372) 377 900
**F:** +40 (372) 333 800
**E:** kpmgro@kpmg.ro

#### Constanța

Blv. Mamaia nr. 208, Etajul 4,
Constanța, 900540
**T:** +40 (756) 070 044
**F:** +40 (752) 710 044
**E:** kpmgro@kpmg.ro

#### Iași

Ideo Business Center
Șoseaua Păcurari nr. 138, Parter,
Iași, 700522
**T:** +40 (756) 070 048
**F:** +40 (752) 710 048
**E:** kpmgro@kpmg.ro

#### Timișoara

ISHO Offices
Blv. Take Ionescu nr. 50,
Clădirea A, Etaj 7,
Timiș, 300222
**T:** +40 (372) 377 999
**F:** +40 (372) 377 977
**E:** kpmgro@kpmg.ro

### KPMG în Moldova

Blv. Stefan cel Mare nr. 171/1,
Etaj 8, Chișinău, MD-2004
**T:** +373 (22) 580 580
**F:** +373 (22) 540 499
**E:** kpmg@kpmg.md

www.kpmg.md

### kpmg.com/socialmedia