



INSPECTORATUL DE POLIȚIE JUDEȚEAN BRAȘOV BIROUL ANALIZA ȘI PREVENIREA CRIMINALITĂȚII

TU ȘTII CE FACE COPILUL TĂU PE INTERNET? SETEAZĂ SIGURANȚA COPILULUI TĂU !

Ce măsuri puteți lua pentru a vă proteja copiii în mediul digital și pe rețelele sociale? Privind potențialele amenințări, utilizarea rețelelor sociale poate părea o activitate periculoasă. Cu toate acestea, interdicția de a le folosi nu va rezolva problema - copiii vor găsi o modalitate de a face ceea ce le place.

În schimb, puteți să vă adaptați comportamentul în online pentru a face utilizarea internetului rețelelor sociale mai sigură pentru copiii și familia dumneavoastră.

Pentru a preveni victimizarea în mediul online, Poliția Brașov vă recomandă:

⇒ Păstrați permanent deschise canalele de comunicare cu copiii - dialogul este una dintre cele mai importante componente pentru menținerea copiilor în siguranță în mediul online, mai ales când vorbim despre rețelele sociale. Menținerea unei comunicări deschise și sincere cu copiii dvs. este importantă, dacă vreți ca aceștia să aibă încredere în judecata dvs. și să vă urmeze sfaturile. Un bun exemplu este **cyberbullying**-ul și prevenirea acestuia. Spuneți-i clar copilului că hărțuirea cibernetică este complet inacceptabilă, indiferent dacă sunt ei înșiși vizați sau dacă sunt tentați să participe la atacarea altora. Când se confruntă cu un astfel de comportament, chiar dacă nu îi privește în mod direct, ar trebui să anunțe imediat pe cineva - pe dvs., un profesor sau alți adulți responsabili.

⇒ Utilizați aplicații de **control parental** - în funcție de vârsta copiilor dvs., puteți utiliza software-ul de control parental pentru a seta o listă de site-uri web sau aplicații blocate și pentru a restricționa orele la care copilul dvs. poate fi prezent online. De asemenea, puteți oferi copilului dvs. acces complet la tot ce este online, cu monitorizare încorporată, care vă permite să vedeți ceea ce vede copilul. Copilul dvs. ar trebui să facă parte din procesul de luare a deciziilor. Dacă alegeți să le limitați accesul sau timpul online, software-urile de control parental le permit copiilor să vă solicite, în timp real, permisiunea de a vizita anumite site-uri web sau de a beneficia de timp suplimentar petrecut pe rețelele sociale. Amintiți-vă: doriți să încurajați discuțiile despre importanța

echilibrării timpului petrecut pentru socializare online cu alte obligații ale copiilor, cum ar fi efectuarea temelor pentru acasă.

⇒ **Utilizați protecția anti-spam și firewall** - Este recomandată instalarea pe dispozitivele copilului dvs. a unei soluții de securitate cu capacități de detectare proactivă, pentru a evita programele malware, ransomware (*ransomware*: este un software rău intenționat care, după ce se instalează pe dispozitivul victimei - calculator, smartphone, criptează datele victimei ținându-le „ostatic”, sau șantajează victima, pe care o amenință că îi va publica datele dacă aceasta nu plătește o „răscumpărare” -în engleză “ransom”) . De cele mai multe ori, ransomware-ul păcălește victima, spunându-i că s-a găsit activitate ilegală pe dispozitiv și că trebuie să plătească o sumă de bani ca să recapete controlul asupra dispozitivului., tentativele de phishing etc., atunci când utilizați rețelele sociale. Asigurați-vă că soluția pe care o alegeți include protecție antispam și firewall.

⇒ **Utilizați parole puternice !** Copiii dvs. știu cum arată o parolă sigură? Greu de crezut, dar, chiar și unii adulți încă folosesc elemente ușor de ghicit, precum cuvântul „parolă” sau șirul de cifre „12345”! Parolele copilului dvs. trebuie să conțină cel puțin 12 caractere, care să includă litere mari și mici, un număr și un simbol special (# sau @). Amintiți-le copiilor să nu-și împărtășească parolele cu nimeni, nici măcar cu cei mai buni prieteni!

⇒ **Utilizați autentificarea în doi pași!** Când se conectează copiii pe rețelele sociale, asigurați-vă că se folosește opțiunea de verificare cu doi factori (în doi pași) oferită în setările de securitate. Cunoscută și sub denumirea de *autentificare cu doi factori*, această metodă adaugă un alt nivel de securitate, greu de compromis de către atacatori, trimițându-i copilului o parolă unică pe care să o introducă de fiecare dată când se conectează sau utilizează un dispozitiv în care nu are încredere. Puteți configura acest lucru împreună și să discutați de ce este important ca numai utilizatorul autorizat să poată accesa un cont. Dacă altcineva intră în contul copilului, ar putea să șteargă informații, să adauge fotografii sau mesaje nepotrivite, să-l agreseze cibernetic sau chiar să încerce să-i fure identitatea.

⇒ **Schimbați setările profilului în “mod privat”!** Setările implicite de confidențialitate pentru rețelele sociale nu vor garanta siguranța copilului dvs. Pentru început, profilurile ar trebui să fie setate pe opțiunea “*privat*” în loc de “*public*”. Pentru exemplificare, vom folosi platforma Instagram și un telefon mobil: conectați-vă la profilul copilului dvs. atingând pictograma “*persoană*”. Glisați spre stânga și atingeți pictograma “Setări” (de obicei, pictograma

respectivă este o rotiță dințată). Selectați “Confidențialitate și securitate”, apoi “Confidențialitatea contului”, după care activați “Contul privat”.

■ Câteva recomandări pentru utilizarea în siguranță a rețelelor sociale!

⇒ Învățați copilul:

- să nu facă publice, vreodată, date personale precum adresa de acasă, numele școlii la care învață sau numărul de telefon, nici al său, al dvs. sau al rudelor, prietenilor etc.

- să folosească chat-uri, mesagerii instant sau rețele de socializare online adecvate vârstei sale și să comunice doar cu persoane apropiate vârstei sale, cu prieteni pe care îi cunoașteți și dvs. sau cu membri ai familiei.

- să folosească webcam-ul pentru a comunica exclusiv cu oameni pe care îi cunoașteți și dvs. în viața reală și să închidă camera atunci când nu o folosește.

- să nu dea curs, niciodată, unor solicitări de a se întâlni în viața reală cu persoane cunoscute online. Dacă chiar îi place cu adevărat de cineva cunoscut online și vrea să se întâlnească cu el/ea, să vă anunțe și pe dvs. eventual, ca să participați la prima întâlnire.

- să nu accepte vreodată cereri de prietenie de la persoane pe care nu le cunoaște în viața reală, în cadrul unei rețele de socializare online, precum Instagram, TikTok sau Facebook, decât dacă acestea i-au fost recomandate de părinți sau prieteni de încredere.

- să nu pună în circulație mesaje vulgare, imagini sau alte materiale cu el sau cu alți cunoscuți în ipostaze indecente.

- să nu răspundă la mesaje menite să-l hărțuiască, și să blocheze expeditorii unor astfel de mesaje.

- să se deconecteze de la internet, atunci când nu îl folosește.

- să respingă și să blocheze mesaje sau contacte nedorite.

⇒ **Ajutați-vă copilul să înțeleagă și să accepte faptul că nu poate (și se poate dovedi chiar periculos) să instaleze aplicații sau să-și creeze conturi pe rețelele de socializare fără acordul dvs!** Aceasta nu trebuie văzută ca o formă de cenzură exercitată de părinte, ci ca o măsură de protecție a copiilor în activitățile lor online. Cu alte cuvinte, înainte de a da click pe linkuri sau butoane de descărcare a unor

aplicații, să se gândească dacă nu e periculos și, eventual, să vă ceară sfatul și sprijinul.

- ⇒ Nici în viața reală, nici în mediul online, oamenii nu sunt întotdeauna cei care pretind că sunt. Ajutați-vă copilul să învețe să comunice prudent în mediul online, să nu divulge mai multe informații decât este cazul și, în niciun caz, să nu dea informații cerute de necunoscuți.
- ⇒ Securizați profilul conturilor copilului dvs., ajustând setările de confidențialitate, pentru a vă asigura că informațiile și fotografiile pe care acesta le diseminează pe internet sunt văzute doar de prieteni și de persoane de încredere.
- ⇒ Aflați exact ce –site-uri de socializare folosește copilul, pe cine are în lista de prieteni (repetăți, împreună cu el, recomandările noastre de mai sus).
- ⇒ Folosiți firewall-ul și alte programe de securitate online pentru a bloca site-urile cu conținut neadecvat pentru copii.
- ⇒ Monitorizați constant activitatea online a copilului (restricționați accesul la programe, softuri și site-uri care i-ar putea face rău) !