



ENJOY SAFER TECHNOLOGY™

safer**kidsonline**

**Cum facem din
internet un loc mai
sigur pentru copii -
ghid pentru părinți**

Vieți digitale

Mulți dintre cei care ne-am ocupat de acest ghid suntem la rândul nostru părinți. Simțim nevoia să ne ghidăm copiii pentru ca ei să treacă prin viață cât mai lin și să îi protejăm pe cât posibil, însă în zilele noastre această responsabilitate a devenit o provocare imensă.

Fiind înconjurați de dispozitive mobile din ce în ce mai complexe, cu tot mai multe platforme noi de comunicare și cu un limbaj online în continuă evoluție, părinții trebuie să țină permanent pasul pentru a-și îndruma copiii.

Acest ghid vă oferă o mână de ajutor și vă explică ce trebuie făcut pentru a vă asigura că cei mici pot utiliza internetul în siguranță.



Cine ar trebui să vorbească cu ei?

Oricât de incomod ar putea să pară, acea persoană trebuie să fie chiar un părinte.

Copiii dvs. vor întâlni de-a lungul vremii multe persoane cu un rol important: rude, prieteni sau profesori. Cu toate acestea, niciunul dintre ei nu poate să-și asume rolul de părinte. În ochii unui copil, părintele este cel care deține toate răspunsurile și este capabil să îl ajute în orice situație.

Când ar trebui să vorbiți cu copiii?

Chiar acum!

Din primul moment în care un copil manifestă interes pentru tableta, smartphone-ul sau computerul dvs., ar trebui să începeți să-i explicați cum funcționează lucrurile. Există multe reguli pe care le insuflăm copiilor pentru a rămâne în siguranță în lumea reală. Bineînțeles, există la fel de multe pentru lumea online. În timp ce amenințările imediate la adresa securității personale pot apărea într-o formă diferită, potențialul de a crea pagube este cât se poate de real. Pe măsură ce copilul va crește, vor apărea noi situații cu care trebuie să se confrunte și trebuie să fim pregătiți pentru toate acestea. O abordare caldă și afectuoasă se poate dovedi a fi cea mai utilă, conducând copilul într-o direcția bună.

Educația - un drum cu două sensuri, nu o stradă cu sens unic

Simțiți că cei mici știu mai multe despre tehnologie decât dvs.?

Nu sunteți singurul. În zilele noastre, copiii sunt nativi digitali și sunt capabili să utilizeze noi tehnologii fără îndrumarea celorlalți. Mulți adulți, în schimb, trebuie să antreneze astfel de competențe.

În același timp, este simplu să navigăm pe internet, dar oare știm să o facem în siguranță? Adulții nu au nevoie să știe mai multe decât copiii despre lumea virtuală, însă ar trebui să poată da sfaturi în cazul în care copilul întâmpină situații bizare pe internet.

Important este ca cei mici să se simtă la rândul lor incluși: creați un mediu în care să poată puna întrebări liber și să poată accesa oricând informații noi.

Ce trebuie să faceți când copilul ajunge la „vârsta aceea”?

Folosiți instrumente de control parental

Indiferent care e vârsta copiilor, puteți să vă bazați pe o tehnologie deja existentă. Instrumentele de control parental ESET fac posibilă blocarea site-urilor sau chiar a categoriilor de pagini ce promovează conținut nepotrivit vârstei. Puteți seta limite de timp pentru navigarea pe internet sau pentru jocuri. În același timp, un astfel de instrument îi permite copilului să vă ceară permisiunea de a vizita anumite pagini sau de a avea mai mult timp alocat jocurilor, dacă și-au terminat temele.

Pe lângă astfel de instrumente, avem câteva sfaturi pentru diferite grupe de vârstă, care vor face activitățile lor online mai sigure.

Copii de până în 10 ani

1. Ghidați-i în primele lor experiențe pe web.

Asigurați-vă că sunteți acolo când micuții dvs. fac primii pași în lumea digitală. Primul contact pe care îl are un copil cu internetul este o bună ocazie de a stabili câteva reguli de bază și de a-i ghida în noua lor aventură.

2. Stabiliți condițiile pentru utilizarea sigură a internetului

Stabiliți câteva reguli simple pentru utilizarea internetului. O idee bună ar fi să monitorizați în primă fază numărul de ore petrecut online de cel mic și să setați o limită de timp în care îi este permis accesul la internet.

3. Fiți un bun exemplu

Copiii copiază, de obicei, comportamentul părinților, iar acest lucru se aplică și în mediul online. Dacă membrii familiei au o conduită bună, este probabil ca un copil să le urmeze exemplul.



Între 11-14 ani

1. Sfătuiți-i să nu împărtășească informații personale

Este important să facem copiii să înțeleagă că nu toate persoanele din lumea virtuală vor să ne fie prieteni și că unii ar putea avea chiar intenții ascunse. Explicați-le de ce nu este sigur să-și împărtășească datele personale, cum ar fi adresa, numărul de telefon, școala sau after-school-ul la care merg. De asemenea, ar fi bine să vă fie cerut sfatul înainte de a posta imagini pe internet.

2. Mențineți un dialog deschis

Încurajați copiii să fie deschiși cu dvs. și să vă întrebe liber orice. Dacă utilizați un computer desktop, încercați să îl instalați într-o cameră în care vă petreceți timpul cu toții și unde poate fi sub supravegherea dvs., nu în dormitorul personal.



Între 15 și 18 ani

1. Nimeni altcineva nu ar trebui să cunoască parolele copiilor

Știm că adolescenții pot fi dificili, dar asigurați-vă că înțeleg și că pun în aplicare câteva simple practici atunci când vine vorba de parole. Respectați-le intimitatea, dar, în același timp, asigurați-vă că nu-și împărtășesc parola cu un străin sau alte persoane.

2. Acționați imediat în cazul unei urmăriri sau cyberbullying

Vă mai amintiți de bătăușul școlii? Copilul care le făcea viața mai grea colegilor? În zilele noastre, astfel de „bătăuși” s-au mutat în mediul digital și se ascund în spatele computerului. Ceea ce nu s-a schimbat, însă, este faptul că încearcă să le facă rău celorlalți, cel puțin la nivel psihologic. Prin urmare, ar fi bine ca părinții să fie informați imediat despre astfel de tentative de hărțuire online.

3. Tranzacțiile financiare online sunt destinate doar adulților

Achizițiile online nu ar trebui să fie o problemă, câtă vreme sunt făcute cu atenție. Până când copiii nu vor înțelege măsurile de precauție necesare care trebuie luate la folosirea datelor financiare personale, ei ar trebui să facă acest lucru numai sub supravegherea părinților.



Care sunt principalele amenințări online?

Malware

„Malware” este prescurtarea de la „malicious software” (software malițios). Acest tip de aplicație încearcă să compromită un dispozitiv în diverse moduri. Unele dintre ele vor cripta fișiere de pe computerul dvs., altele vor încerca să vă spioneze sau să descarce alte aplicații periculoase pe computer.

În majoritatea cazurilor, infecția are loc din cauza „greșelilor” comise de utilizatori după ce au fost păcăliți de atacatori. Instalarea unei soluții de securitate și adoptarea câtorva bune practici vor reduce riscul de a fi infectat de acest tip de cod rău intenționat.

Spam

Sigur v-ați mai întâlnit cu mesaje spam. Sunt acele e-mailuri nesolicitate, care continuă să apară în căsuța de e-mail. Aceste mesaje includ de obicei reclame care vă invită să vizitați anumite pagini cu oferte „miracol” și conțin în mare parte conținut potențial dăunător.

Scam

Scamurile sunt acte de înșelătorie derulate pe internet. Ele pot lua inițial mai multe forme, cum ar fi spamul și utilizarea unor tehnici de inginerie socială, caz în care atacatorii se oferă să vă vândă ceva, să impersoneze un coleg sau chiar o instituție bancară, doar pentru a ajunge la datele dvs. personale. Mesajele false care solicită numele de utilizator și parolele conturilor de pe rețelele sociale sunt, de asemenea, un exemplu frecvent de înșelătorie.

Hărțuirea online (cyberbullying)

Acest comportament ostil are ca țintă, de regulă, copiii. Victima poate fi amenințată și umilită de către persoane din mediul online, fenomen des întâlnit în rândul adolescenților. Astfel de situații le pot chiar provoca traume emoționale victimelor. Hărțuirea online se poate manifesta sub multe forme: în unele cazuri, poate avea loc chiar în fereastra de chat din diferite jocuri video.

Grooming

Grooming-ul apare atunci când un adult încearcă să convingă un copil să întrețină diferite activități sexuale. Un groomer încearcă să câștige încrederea copilului și să construiască o legătură emoțională cu acesta. Aceste persoane se pot da drept copii pentru a stabili o relație strânsă cu cei mici și încearcă apoi să organizeze o întâlnire în viața reală. Pentru un părinte este important să știe în permanență cu ce persoane intră în contact cei mici în mediul virtual.

Sexting

Termenul de „sexting” este derivat din „sex” și „texting” și e un concept care există deja de ceva vreme. Funcția SMS a fost utilizată inițial pe telefoanele mobile pentru a conversa prin mesaje text, însă evoluția tehnologiilor de emailing și de mesagerie a făcut posibilă mai târziu trimiterea de fotografii și clipuri video. Este o practică obișnuită în rândul adolescenților și copiilor, acum că dețin permanent acces la dispozitivele mobile.

Furtul de informații

Informațiile trimise pe web, fără a ține de cont de diferite măsuri de precauție, pot fi interceptate de persoane terțe. Informațiile obținute în acest mod pot fi utilizate în scopuri precum furtul de identitate sau șantaj.



Concluzii finale

Folosiți instrumente de control parental

Acestea pot fi utilizate în browsere și software antivirus. Cea mai recentă versiune a soluției noastre ESET Internet Security vine la pachet cu un astfel de instrument sau puteți apela oricând la o aplicație separată precum ESET Parental Control pentru Android. Acest tip de instrumente sunt disponibile și pentru consolele de jocuri.

Nu lăsați copilul să trimită informații confidențiale pe internet

Informațiile sensibile nu ar trebui solicitate niciodată prin e-mail sau chat. Băncile nu vor solicita niciodată sub această formă datele bancare sau codul PIN. De asemenea, este important să nu le oferiți copiilor informații atât de valoroase.

Nu răspundeți și nu încercați să eliminați mesajele primite de la hărțuitori

În cazul în care copilul dvs. se confruntă cu cyberbullying, ar fi indicat să nu ripostați. Explicați-le că persoana din spatele unor astfel de acțiuni așteaptă întocmai o reacție, deoarece le hrănește dorința de a face rău altora. Dacă întâmpinați o astfel de situație, anunțați autoritățile competente. Nu ștergeți niciun mesaj primit, deoarece poate fi folosit ca dovadă.



Rămâneți permanent la curent

În zilele noastre, nu este o soluție să le refuzăm copiilor accesul la tehnologie. Dispozitivele digitale fac parte din viața lor de zi cu zi și sunt din ce în ce mai importante în dezvoltarea lor. În loc să impuneți restricții, ajutați-i să folosească astfel de dispozitive în siguranță și luați parte la interacțiunea dintre copil și tehnologie. Nu uitați, de asemenea, că multe dintre aceste riscuri pot afecta și adulții, iar multe dintre precauțiile descrise aici pot fi adoptate la orice vârstă. Siguranța copiilor este responsabilitatea tuturor, iar sfaturile furnizate în acest ghid sunt doar niște pași de bază. Pentru mai multe informații, vizitați site-urile noastre web și paginile de social media.

www.eset.ro

www.blog.eset.ro

<https://saferkidsonline.eset.com/ro>

www.facebook.com/esetromania

www.twitter.com/ESET_RO

www.linkedin.com/company/eset-romania