



Primii pași în siguranță în viața digitală



Primii pași în siguranță în viața digitală
Ghid pentru părinți și educatori realizat de MCSI în
colaborare cu CERT-RO
**Pentru mai multe informații privind securitatea
informatică vizitați pagina www.cert.ro**
Sursa imaginilor: www.openclipart.org



Ghid pentru părinți și educatori



CERT.RO

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE
DE SECURITATE CIBERNETICĂ
ROMANIAN NATIONAL COMPUTER SECURITY
INCIDENT RESPONSE TEAM

VIAȚA DIGITALĂ ȘI RISCURILE LA ADRESA COPIILOR

Categoriile de activități în mediul digital frecvent întâlnite indiferent de vârstă:

- Conectarea și comunicarea cu prietenii și familia;
- Descărcarea de aplicații, documente și conținut multimedia;
- Căutarea de informații și vizualizarea de conținut multimedia;
- Publicarea activităților desfășurate, a locației precum și a fotografiilor și înregistrărilor video;
- Crearea de conturi pe rețelele sociale.

Riscuri principale pentru copii în mediul digital:

- Accesarea de conținut interzis sau impropriu vârstei (pornografie, violență, incitare la ură, etc);
- Contactul cu persoane rău-intenționate (cyber-bullying, exploatare sexuală, escrocherie, etc);
- Adoptarea unei conduite imorale sau angrenarea în activități ilegale;
- Compromiterea datelor și sistemelor informatice și furtul de identitate;
- Pierderi financiare pentru familie.

MĂSURI DE PROTECȚIE CU CARACTER TEHNIC

- Utilizați setările de siguranță pentru Youtube – limitând astfel accesul la conținut neadecvat copiilor
- Ajuțați copiii în stabilirea setărilor de confidențialitate la profilele de pe rețelele sociale
- Instalați programe antivirus pe calculator și dispozitivele mobile
- Creați cont separat de utilizator pentru copii pe calculator și pe dispozitivele mobile.
- Securizați sistemele de jocuri ce permit conectarea online
- Instalați browsere și utilizați motoare de căutare sigure pentru copii
- Utilizați programe de control parental.

Adrese utile pentru setările de confidențialitate a rețelelor sociale mai populare:

- Facebook: <https://www.facebook.com/help/325807937506242/>
- Instagram: <https://help.instagram.com/116024195217477/>
- Snapchat: <https://support.snapchat.com/a/privacy-settings>
- WhatsApp: <https://www.whatsapp.com/faq/en/general/21197244>
- Kik: <https://kikinteractive.zendesk.com/hc/en-us/articles/217680888-How-can-I-keep-my-Kik-account-private->
- Ask.fm: <http://safety.ask.fm/safety-tools/>

RISCURI PRIVIND RELAȚIONAREA ONLINE A COPIILOR

Pericole:

- Contactul cu persoane rău intenționate este extrem de facil.
- Copiii pot cădea victime escrocheriilor, exploatării sexuale, hărțuirii și defăimării online ori se pot lăsa antrenați de către ceilalți în activități dăunătoare ori riscante.

Lecții esențiale:

- În viața de zi cu zi suntem circumspecți cu privire la intențiile persoanelor necunoscute.
- Persoane adulte își pot crea profile de copil pentru a intra în relație cu minori în scopul exploatării acestora.
- Sexting este forma de exploatare prin șantajarea minorului cu publicarea de poze nud ale acestuia.
- Hărțuirea online (cyber-bullying) compromite emoțional victimele, copii putând fi atât victime cât și făptuitori.

Măsurile minime de precauție:

- Nu răspundem cererilor de prietenie și mesajelor de la necunoscuți.
- Nu ne întâlnim cu persoane "cunoscute prin internet"
- Nu trimitem poze în ipostaze sexuale sau nud nimănui.
- Nu ne angrenăm în defăimarea nimănui pe internet.
- Cerem ajutorul părinților și semnalăm situațiile întâlnite.
- Ne protejăm și online la fel ca offline

ÎN PREGĂTIREA INSTRUIRII...

Pentru a-i ajuta pe copii să facă față pericolelor vieții digitale sunt necesare:

- Informarea privind amenințările online în general, dar mai ales cele orientate către tineri;
- Informarea privind abilitățile necesare nouă și copiilor pentru evitarea pericolelor;
- Alegerea celor mai potrivite metode de a transmite copiilor informațiile necesare care să genereze un comportament adecvat în mediul online.

Sfaturi privind măsurile adecvate:

- Inițiați dvs. comunicarea și dialogul deschis pe teme legate de viața online și dificultățile întâlnite.
- Utilizați programe de control parental și securizarea dispozitivelor și conturilor utilizate de copii în mediul online.
- Încercați să înțelegeți modul în care sunt utilizate platformele preferate de copii.

PUBLICAREA DE INFORMAȚII ONLINE

Pericole:

- Publicarea de informații, fotografii sau clipuri video care pot aduce prejudicii reputației, imaginii proprii ori pot cauza suferințe celorlalți.
- Publicarea de date personale (locație, adresă, numere de card de credit, etc.) ce pot fi utilizate de către persoane rău intenționate.
- Promovarea mesajelor de ură, incitare la violență, hărțuire, etc.

Leții de învățat:

- Civismul și morala sunt valabile și online. Tratăm online pe ceilalți așa cum dorim și noi să fim tratați.
- Faptele comise prin internet lasă urme, unele atrag răspunderea penală iar făptuitorii pot fi identificați.
- Similar vieții reale, ne protejăm și online persoana, bunurile și nu dăm informații despre noi necunoscuților.

Măsuri minime de precauție:

- Nu răspundem la provocări și îndemnuri de a comite fapte ilegale ori care pot produce suferință cuiva.
- Nu distribuim fotografii/video cu noi, familia, locuința sau bunurile.
- Cântărim posibilele consecințe negative înainte de a acționa online.
- Anunțăm părinții despre faptele negative observate și cerem ajutorul
- Limităm accesul publicului la profilele și conturile noastre.

ACCESAREA DE CONȚINUT INTERZIS SAU IMPROPRIU VÂRSTEI

Pericole:

- Accesul la materiale cu caracter pornografic ori care incită la violență și ură este facil pe internet ori prin sisteme de file-sharing, chiar fără intenția de a găsi astfel de materiale.
- Similar sunt accesibile materiale ilegale (ex. pornografie infantilă).

De reținut:

- Expunerea la aceste tipuri de informații are consecințe negative asupra dezvoltării psiho-emoționale a copiilor.
- Accesarea, descărcarea, vizualizarea și distribuirea de materiale pornografice cu minori constituie infracțiune.
- Dispozitivele mobile cu acces la internet favorizează accesul necontrolat la astfel de materiale.

Măsuri minime de precauție:

- Dialogul cu copiii este esențial în înțelegerea pericolelor și a consecințelor.
- Dispozitivele mobile date copiilor trebuie prealabil limitate ca acces prin crearea unui cont de utilizator special.
- Este recomandată instalarea de aplicații de control parental.
- Calculatorul "de acasă" trebuie amplasat în zonă vizibilă.

