



ASCPD

Asociația Specialiștilor
în Confidențialitate
și Protecția Datelor



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

CUM ÎMI PROTEJEZ DATELE PERSONALE ȘI MĂ APĂR DE PERICOLE ÎN MEDIUL ONLINE?

***Ghid de conștientizare a importanței protecției
datelor cu caracter personal și a securității
cibernetice pentru copii, părinți, profesori***

AUTORI

DANIELA-IRINA CIREAȘĂ
PREȘEDINTE ASCPD
ASCPD

DANIELA SIMIONOVICI
VICEPREȘEDINTE

COLABORATORI

ALEXANDRA VESE
MEMBRU ASCPD

ANDREI CONONOV
MEMBRU ASCPD

I. INTRODUCERE

Prezentul ghid își propune să trateze subiectul confidențialității (privacy), a protecției datelor (data privacy) și a securității cibernetice (cybersecurity) a copiilor în mediul online.

Securitatea cibernetică sau securitatea online este o modalitate eficientă de a asigura protecția datelor personale, cele două fiind indisolubil conectate într-o eră a digitalizării și a tehnologizării precum cea pe care o trăim în prezent.

Petrecând foarte mult timp online, copiii se confruntă din ce în ce mai mult cu amenințări în acest mediu, cu încălcări ale protecției și confidențialității datelor, cu pericole și cu provocări de securitate cibernetică, inclusiv violență și incidente legate de pedofilie și cyberbullying (bullying prin folosirea tehnologiilor digitale; se poate întâmpla pe rețelele de socializare, pe platformele de schimb de mesaje, pe platformele de jocuri și pe telefoanele mobile - este vorba despre un comportament indezirabil, frecvent, care are scopul de a-i speria, înfuria sau umili pe cei vizați)¹.

Școala online a devenit și ea o realitate a zilelor noastre, acest fapt însemnând o expunere din ce în ce mai mare a copiilor la agresiune și violență în mediul virtual. Este foarte important să existe un echilibru între siguranța elevilor în mediul online în timpul activităților specifice de predare și învățare și activităților extrașcolare, pe de o parte, și efectele contactului cultural direct în comunitate, pe de altă parte.

Conștientizarea riscurilor, pregătirea părinților și comunicarea cu copiii despre protecția datelor cu caracter personal și pericolele din mediul online sunt extrem de importante și sunt complementare activităților desfășurate în școli.

Ghidul reflectă o preocupare sporită pentru dreptul la viața privată a copiilor și pentru interesul superior al acestora, care „se circumscrie dreptului copilului la o dezvoltare fizică și morală normală, la echilibru socioafectiv și la viața de familie”².

Mediul digital nu a fost conceput inițial pentru copii, dar joacă un rol semnificativ în viața acestora, fapt pentru care noi, adulții, trebuie să ne asigurăm că în toate acțiunile privind furnizarea, reglementarea, proiectarea, gestionarea și utilizarea mediului digital, interesul superior al fiecărui copil este un aspect primordial.



Atunci când se ia în considerare interesul superior al copilului, ar trebui să se țină cont de toate drepturile copiilor, inclusiv de dreptul lor de a căuta, de a primi și de a distribui informații, de a fi protejați de eventuale suferințe, jigniri sau insulte la care ar putea fi expuși, de a li se acorda atenția cuvenită tuturor opiniilor pe care aceștia le au, de a se ține cont de dorințele sau/și de alegerile lor în ceea ce privește anumite activități pe care vor să le desfășoare și să li se asigure transparență în evaluarea interesului lor și în criteriile care au fost folosite în această evaluare.³

Mai mult, Regulamentul 679/2016, cunoscut mai ales ca GDPR, îi obligă pe cei care prelucreează date cu caracter personal să furnizeze informațiile legate de prelucrarea datelor personale „într-

1 UNICEF, Cyberbullying: Ce este și cum îi punem capăt? 10 lucruri pe care adolescenții vor să le știe despre cyberbullying. Disponibil la: <https://www.unicef.org/moldova/articole/cyberbullying-ce-este-%C8%99i-cum-%C3%AEi-punem-cap%C4%B3t>

2 Legea nr. 272/2004 privind protecția și promovarea drepturilor copilului, art. 2, alin. 1 și 2: „(1) Prezenta lege, orice alte reglementări adoptate în domeniul respectării și promovării drepturilor copilului, precum și orice act juridic emis sau, după caz, încheiat în acest domeniu se subordonează cu prioritate principiului interesului superior al copilului.

(2) Interesul superior al copilului se circumscrie dreptului copilului la o dezvoltare fizică și morală normală, la echilibru socioafectiv și la viața de familie”. Disponibil la: <https://legislatie.just.ro/Public/DetaliuDocument/156097>

3 United Nations, Convention on the Rights of the Child, pct. B, Interesul superior al copilului

Protecție suplimentară este acordată datelor cu caracter personal ale copiilor, deoarece copiii sunt mai puțin conștienți de riscurile și consecințele partajării datelor și de drepturile lor.

Orice informație adresată în mod special unui copil ar trebui adaptată pentru a fi ușor accesibilă, folosind un limbaj clar și simplu.

Pentru majoritatea serviciilor online este necesar consimțământul părintelui sau al tutorelui pentru a prelucra datele personale ale unui copil până la o anumită vârstă. Acest lucru se aplică site-urilor de rețele sociale, precum și platformelor pentru descărcarea de muzică și cumpărarea de jocuri online.



Companiile (și, în general, orice operator de date, inclusiv școlile) trebuie să depună eforturi rezonabile⁶, ținând cont de tehnologia disponibilă, pentru a verifica situațiile în care consimțământul dat este cu adevărat în conformitate cu legea. Acest lucru poate implica implementarea măsurilor de verificare a vârstei, cum ar fi adresarea unei întrebări la care un copil nu ar putea răspunde sau solicitarea adresată minorului de a furniza e-mail-ul părinților săi pentru a se putea obține acordul scris al acestora.

Articolul 8 din Regulamentul UE nr. 679/2016, privind protecția datelor personale, stabilește condițiile aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale și anume: în cazul oferirii acestor servicii⁷ în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă acesta are cel puțin vârsta de 16 ani.

Dacă vârsta copilul este sub limita de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului. Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri dacă titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.⁸

De asemenea, considerentul (38) din Regulament prevede: *“copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. Această protecție specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de*

⁶ Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, Versiunea 1.1, Adoptate la 4 mai 2020, p 33: “Caracterul rezonabil, atât în ceea ce privește verificarea faptului că un utilizator are vârsta minimă pentru a da consimțământul în nume propriu, cât și în ceea ce privește verificarea faptului că persoana care acordă consimțământul în numele unui copil este titulară a răspunderii părintești, poate depinde de riscurile inerente prelucrării, precum și de tehnologia disponibilă. În cazurile cu risc scăzut, verificarea răspunderii părintești prin e-mail poate fi suficientă. În schimb, în cazurile cu risc sporit, ar putea fi oportun să se solicite mai multe dovezi, astfel încât operatorul să poată verifica și păstra informațiile în temeiul articolului 7 alineatul (1) din GDPR. Serviciile de verificare furnizate de o parte terță de încredere pot oferi soluții care să reducă la minimum volumul de date cu caracter personal pe care operatorul însuși trebuie să îl prelucreze.”. Disponibil pentru download direct, la: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_ro.pdf

⁷ CURIA, HOTĂRÂREA CURȚII (Camera a treia), 15 septembrie 2016, cauza C-484/14, Tobias Mc Fadden împotriva Sony Music Entertainment Germany GmbH: “Serviciile societății informaționale sunt prestate la distanță, electronic și la solicitarea individuală a unui beneficiar al serviciilor. Acestea se referă la o gamă largă de activități economice care se desfășoară online. Serviciile societății informaționale nu se limitează exclusiv la servicii în urma cărora se încheie contracte online, ci, în măsura în care acestea reprezintă o activitate economică, se extind la servicii care nu sunt remunerate de cei care le primesc, cum ar fi serviciile care furnizează informații online ori comunicări comerciale sau cele care furnizează instrumente de căutare, accesare și recuperare a datelor. Serviciile societății informaționale presupun, de asemenea, servicii care constau în furnizarea accesului la o rețea de comunicații etc.”. Disponibil la:

https://curia.europa.eu/juris/document/document_print.jsf?jsessionid=02D734A02B6F26FB4E23F888E5A350C6?docid=183363&text=&doclang=R0&pageIndex=0&cid=1849533

⁸ Regulamentul UE 679/2016, art. 8. Disponibil pentru download direct aici: <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EL>

Ghid (digital) de conștientizare a importanței protecției datelor cu caracter personal și a securității cibernetice pentru **copii**



Instagram

Înscrie-te pentru a vedea fotografiile
și videoclipurile prietenilor tăi

CONECTAȚI-VĂ CU FACEBOOK

SAU

NUMĂR DE TELEFON SAU EMAIL

NUME ȘI PRENUME

NUMELE UTILIZATORULUI

PAROLĂ

ÎNSCRIE-TE

Prin înscriere, sunteți de acord
cu termenii și condițiile noastre

CREAZĂ UN NOU CONT

NUME PRENUME

NUMĂR DE TELEFON SAU EMAIL

PAROLĂ NOUĂ

DATA NAȘTERII

LUNA ZIUA ANUL

GEN

FEMININ MASCULIN

Pagina de creare cont pe site-ul Instagram, sunt solicitate date personale cum ar fi numele și prenumele, numărul de telefon sau adresa de e-mail, data nașterii și sexul



Știi că?

Orice informație care te poate identifica clar, sau care poate ajuta la identificarea cuiva, este considerată dată personală. Acest lucru include și numele prietenilor tăi, numerele lor de telefon, adresele de e-mail și chiar informații despre persoana care îți place. Prin urmare, orice informație despre tine trebuie protejată ca dată personală!



Știi că?

Există și date personale considerate „speciale”? Legea ne obligă să protejăm acest tip de date în mod deosebit. În categoria datelor speciale intră: datele privind starea ta de sănătate, amprentele și conformația irisului din ochiul tău (sau alte date biometrice), date care pot spune dacă ești român sau rrom, asiatic sau african, confesiunea religioasă, opiniile politice, datele tale genetice, precum și date despre viața sau orientarea ta sexuală.

Prin conștientizarea securității cibernetice, putem fi ca niște mici detectivi ai internetului, pregătiți să ne apărăm și să protejăm lumea noastră digitală de orice pericol care ne-ar putea afecta. Astfel, putem să ne bucurăm de internet în siguranță și să ne jucăm fără griji!

II.1.5. La ce sunt folosite datele tale personale?

Datele personale pot fi folosite în moduri periculoase. De exemplu, cineva ar putea să le folosească pentru a crea documente false sau pentru a intra în conturile tale online.¹⁴



Alteori, datele personale pot fi folosite pentru furtul identității noastre financiare, adică cineva ar putea să ne fure banii din cont. Aceasta înseamnă că cineva ar putea să obțină informații despre cardurile bancare și să le folosească în mod ilegal.

Mai există și situații în care datele personale sunt folosite pentru a crea identități online false. De exemplu, cineva ar putea să creeze un cont fals pe internet folosind informațiile tale, care să lase impresia că ești tu, dar, de fapt, să-i poată păcăli pe alții, fără să riște să fie descoperit, folosind datele culese ca să facă rău altora și să comită tot felul de ilegalități.

Este important să fim atenți la cine are acces la datele noastre și să luăm măsuri pentru a ne proteja informațiile personale.

Hai să vedem dacă ai înțeles informațiile pe care ți le-am dat până acum:

Securitatea cibernetică ne protejează datele și activitățile online de furt și alte amenințări. Este important să păstrăm informațiile personale în siguranță, pentru a evita jocurile și site-urile inadecvate și pentru a preveni contactul cu persoanele răuvoitoare. Conștientizarea securității cibernetice înseamnă învățarea modului în care să ne protejăm pe internet, să fim atenți la pericole și să evităm situațiile de risc.

II.1.6. Gândește înainte de a da click!

Dacă prietenii, părinții sau profesorii tăi văd postările tale, vor avea o impresie bună despre tine? Va fi cineva jignit sau trist din cauza postărilor tale? Dacă ai cea mai mică îndoială că postările tale ar putea fi înțelese greșit, atunci nu posta. Fii responsabil! Online, totul poate fi partajat (sau share[d]-uit, ca să folosim un termen la modă, cu care, probabil, ești mai obișnuit), căutat, dar, mai ales găsit. Nimic nu este, niciodată, șters cu adevărat. Internetul ne aduce mai aproape și, în zilele noastre, poți oricând să vorbești cu cei dragi, aflați la distanță. În trecut, părinții tăi trebuiau să aștepte săptămâni, sau chiar luni, pentru a primi o scrisoare, cu sau fără fotografii. Acum, este nevoie doar de câteva secunde pentru a posta și a primi sau a trimite poze.

Dar ...

Tot trebuie să fii atent! Există și alți oameni, în afară de familia și prietenii tăi, care pot vedea ceea ce postezi și pot descărca sau chiar distribui informațiile tale. Tot ce postezi conține informații despre tine!



¹⁴ Wikipedia, *Date personale*. Disponibil la: https://ro.wikipedia.org/wiki/Date_personale

O altă consecință legată direct de cazul prezentat de noi este cea în care datele făcute cadou de către Twitter ar putea, la un moment dat, să devină publice și accesibile oricui. Prin urmare, ceva ce ai postat în copilărie pe Twitter și ți s-a părut inofensiv, ba ai mai și uitat că ai postat acele informații, este posibil să se întoarcă împotriva ta (sau a altora), ca adult.

Adrese de e-mail “gratuite”

Așa cum am precizat mai sus, nimic nu e gratuit. Când schimbi e-mail-uri cu prietenii și pui și atașamente, chiar dacă și tu, și prietenul tău ștergeți mesajele, cu tot cu atașamente, acestea pot rămâne stocate pe serverele respectivelor companii, în locații despre care tu nu știi nimic. Problema este că, așa cum am mai precizat, este aproape o imposibilitate tehnică să faci să dispară complet și definitiv ceva ce ai postat în mediul online. Prin urmare, și conținutul acelor mesaje pe care tu și prietenul tău le-ați șters, ar putea, în orice moment, să apară în spațiul public.

Rețelele de socializare

Pe rețelele de socializare, lucrurile sunt și mai periculoase, deoarece acolo oricine are acces imediat la orice postezi tu. Dacă ai postat ceva ce realizezi că e greșit, sau ți-ar putea produce neazuri, oricât de repede te-ai mișca, există riscul ca acea greșeală să fie deja preluată și “rostogolită” de alții, ca un bulgăre de zăpadă care crește mare-mare și nu-l mai poți opri, oricât ai încerca. Sau, chiar dacă ce ai postat nu este o greșeală în sine, informația respectivă ar putea fi preluată de răuvoitori, exagerată, răstălmăcită, răsucită și prezentată distorsionată, în așa fel încât să poată fi folosită împotriva ta și să-ți facă rău.

Ce poți face?

- Tu ești prima și cea mai importantă linie de apărare, a ta, împotriva a orice ți s-ar putea întâmpla rău pe internet. Ce înseamnă asta? Înseamnă că doar tu te poți păzi, având grijă ce postezi în online. Nu te gândești doar la satisfacția și plăcerea de moment, pe care le simți când postezi ceva, ci încearcă să te gândești dacă nu cumva ceea ce ai postat ar putea fi folosit împotriva ta (să fii bârfit, jignit, umilit, amenințat etc.). **NU uita că orice ai postat public este la dispoziția oricui, poate fi descărcat, copiat, modificat, trucat, refolosit etc., nu doar atunci, ci chiar și peste ani de zile!**
- Stabilește cu mare atenție și responsabilitate cui permiți să aibă acces la informațiile tale pe care le publici pe diverse pagini web și în diverse aplicații (fii foarte atent la setările de confidențialitate). Un like (“îmi place”/thumb up), sau un dislike (“nu-mi place”/thumb down) la o anumită postare îți poate aduce aprecieri de la cei care sunt de acord cu aprecierea/deprecierea ta, dar, în foarte multe cazuri, poate genera o undă de comentarii răutăcioase la adresa ta, sau poate declanșa situații mai grave, cum ar fi cyberbullying. Asta nu înseamnă că nu mai ai voie, sau trebuie să-ți fie teamă să mai exprimi opinii personale, indiferent sub ce formă, în mediul online, ci că trebuie să te gândești bine înainte de asta și să analizezi și consecințele și să iei atitudine doar când ești convins că îți poți asuma respectivele consecințe.
- **Dacă ai publicat postări care nu-ți mai plac, sau s-au dovedit dăunătoare pentru tine, elimină-le imediat!** Chiar dacă nimic nu dispare definitiv din online, cel puțin te elimini pe tine ca sursă primară, principală a respectivelor informații (măcar nu se mai găsesc pe pagina/postarea ta).
- Trăiește momentul, clipa, bucură-te de viață, dar lasă un ochi să privească spre viitor și fii prevăzător, întrebându-te, mereu, înainte de a posta, dacă nu cumva ceea ce vrei să faci s-ar putea dovedi dăunător, pentru tine sau pentru alții, nu neapărat atunci, pe moment, ci chiar și mai târziu.

- Numere naționale unice de identificare (cum ar fi CNP-ul), salvate în documente sau fotografii;
- **Mesajele** text conținând oricare din datele enumerate mai sus și/sau preferințele tale în orice domeniu (această ultimă categorie de date personale sunt extrem de căutate ca să îți se trimită reclame personalizate);
- **Numerele** apelate sau de la care primești apeluri telefonice;
- **Nume, adrese** și numere de telefon salvate în lista de contacte, în browser, în listele de contacte din diverse aplicații etc.;
- **Site-urile** vizitate recent. Deținătorii acestor site-uri, precum și partenerii lor, sunt foarte interesați de istoricul căutărilor/achizițiilor tale și, prin intermediul cookie-urilor obțin o multitudine de informații despre tine pe care le folosesc pentru a obține un câștig direct de la tine sau, indirect, vânzându-le altora etc.¹⁶;
- **Locațiile** în care te-ai aflat recent, care sunt extrase din aplicațiile de navigare folosite de tine sau din fotografii;
- **Locația actuală**, mai ales dacă folosești funcția “share location” a telefonului tău sau din aplicații precum WhatsApp, sau alte aplicații care oferă această funcție (ex.: “Find My Friends”, care este o aplicație disponibilă în “Apple Store”¹⁷ utilizatorilor de iPhone sau celor care folosesc dispozitive cu sistem de operare IOS);
- **Fișiere** accesate recent și care conțin informații despre tine, sau despre alții;
- **Fișiere șterse**. Toate fișierele șterse, chiar și cele care nu mai sunt în coșul de gunoi (Recycle Bin), pot fi recuperate până în momentul rescrierii fizice a echipamentului - momentul în care se formează dispozitivul, adică se șterge tot și se pregătește dispozitivul pentru utilizare, sau ștergerea se face prin scrierea, în sens IT, a unor informații peste cele deja existente, în așa fel încât acestea din urmă să devină imposibil de recunoscut și utilizat.

De fiecare dată când joci jocuri online, discuți pe chat video sau navighezi pe web de pe un telefon mobil sau tabletă, accesezi internetul. Așadar, trebuie să fii atent când folosești telefonul mobil, la fel cum ești atent când folosești un computer, poate chiar mai atent, dată fiind mobilitatea acestui dispozitiv, deoarece faptul că-l poți lua peste tot cu tine înseamnă că îl poți pierde, sau îți poate fi furat la fel de ușor.

Câteva sfaturi pentru a fi în siguranță atunci când folosești un telefon mobil

Iată câteva sfaturi importante pentru a-ți proteja datele și intimitatea atunci când folosești telefonul mobil:¹⁸

1. **Protejează telefonul cu parolă:** Setează o parolă sau un cod PIN pentru a bloca accesul la telefonul tău. Optează pentru o parolă complexă și evită parolele ușor de ghicit.
2. **Setează blocarea automată:** Asigură-te că dispozitivul tău se blochează automat după o perioadă scurtă de inactivitate, pentru a preveni accesul neautorizat.
3. **Instalează un software de securitate (ex. antivirus):** Utilizează aplicații de securitate care te protejează împotriva malware-ului și a altor amenințări cibernetice.
4. **Descarcă aplicații doar din surse verificate:** Instalează aplicații doar din magazinele oficiale de aplicații, cum ar fi Google Play Store sau App Store, și verifică întotdeauna recenziile și permisiunile aplicațiilor.

¹⁶ Wikipedia, Cookie: “Un cookie HTTP sau un modul cookie este un text special, deseori codificat, trimis de un server unui navigator web și apoi trimis înapoi (nemodificat) de către navigator, de fiecare dată când accesează acel server. Cookie-urile sunt folosite pentru autentificare, precum și pentru urmărirea comportamentului utilizatorilor; sunt folosite mai ales reținerea preferințelor utilizatorilor și implementarea sistemului de „coș de cumpărături”. Disponibil la: <https://ro.wikipedia.org/wiki/Cookie>

¹⁷ Apple Store este un magazin online care vinde, sau pune gratuit la dispoziție, aplicații care pot fi instalate pe dispozitive Apple (Iphone, MacOS etc.). Pentru dispozitivele care folosesc sistem de operare Android, “omologul” Appstore este Google Play (n.a.)

¹⁸ certSIGN, “10 trucuri pentru securizarea telefonului mobil”. Disponibil la: <https://www.certsig.ro/ro/10-trucuri-pentru-securizarea-telefonului-mobil/>

dacă printre aceste informații sunt colectate și date personale sensibile (cum ar fi datele despre starea ta de sănătate) pot avea un impact asupra dreptului tău la confidențialitate.

Tehnologiile AI pot ajuta medicii să stabilească corect un diagnostic și să-ți indice tratamentul cel mai potrivit pentru boala ta. Cu toate acestea, dacă aceste tehnologii sunt dezvoltate în grabă, fără a implica sau a lua în considerare diverse setări de securitate, pot avea și consecințe nedorite.

Sistemele AI îți pot recomanda pe cine să urmărești sau cu cine să te împrietenești pe rețelele de socializare (de cine ai mai putea fi interesat, analizând datele tale, dar și ale celorlalte persoane cu care tu ai putea avea ceva în comun, cel mai adesea activități sau hobby-uri despre care ai postat), sau ce melodii să asculți.

Voi, copiii de astăzi, sunteți prima generație care nu-și va aminti niciodată vremurile de dinainte de apariția smartphone-ului. Sunteți prima generație a cărei îngrijire a sănătății și educație sunt din ce în ce mai mult făcute cu ajutorul unor aplicații și echipamente controlate de AI, iar unii dintre voi veți fi primii care vor circula în mașini autoconduse (este puțin impropriu spus "autoconduse", deoarece aceste mașini sunt conduse de AI).

Voi sunteți, de asemenea, generația pentru care riscurile legate de AI, cum ar fi creșterea decalajului digital între femei și bărbați, sau între comunități cu niveluri de dezvoltare economică diferită, automatizarea locurilor de muncă și încălcările confidențialității datelor voastre personale, trebuie abordate înainte ca tehnologiile AI să devină și mai implicate în viitorul vostru.

Acest lucru este deosebit de important, deoarece impactul pe care tehnologiile bazate pe AI îl poate avea asupra copiilor nu este întotdeauna foarte clar.¹⁹ Te încurajăm să accesezi Internetul ca să obții mai multe informații despre inteligența artificială.²⁰

II.1.11. Cum poți face navigarea pe internet sigură?

Nimic nu este sigur în totalitate, nici mersul pe stradă și nici navigarea pe internet. Dar, asta nu înseamnă că nu trebuie să facem tot ce putem să ne trăim viața cât mai în siguranță. De aceea, cel puțin în ceea ce privește navigarea sigură pe internet, îți facem unele recomandări²¹:

- **NU** oferi persoanelor cunoscute pe internet informații despre tine sau despre familia ta, cum ar fi nume: vârstă, număr de telefon, fotografii, adresa de acasă, școala/liceul la care înveți, locul de muncă al părinților, rudelor sau cunoscuților tăi etc.;
- **NU** permite accesul necunoscuților la profilul tău, fii foarte atent ce fotografii, cu tine și/sau cu familia ta, postezi online și, mai ales, **NU** uita că fotografiile sau filmulețele, odată "eliberate" în mediul online, **NU** mai pot fi șterse niciodată, în totalitate, chiar dacă tu le "dai jos" de unde le-ai postat prima dată;
- **NU** te grăbi să crezi că tot ce citești sau vezi pe internet ar fi adevărat. O pagină web se creează foarte ușor și se pot posta cu mare ușurință texte sau imagini/video înșelătoare ("Nu tot ce zboară se mănâncă!"), spune un înțelept proverb românesc). Verifică informațiile din mai multe surse, înainte de a decide să le crezi;
- **NU** fura munca altora de pe internet! Când folosești materiale de pe internet (texte, imagini, video etc.), indică sursa (pagina web) de unde le-ai luat. În acest fel, respecti munca altora și nici nu riști să fii considerat plagiator (hoț), sau creator/distribuitor de știri false (în cazul în care materialele pe care le-ai luat se dovedesc a fi știri/materiale false);
- **NU** dezvălui parolele tale nimănui, nici măcar celui mai bun prieten. Dacă ai cel mai mic dubiu că ți-au fost compromise parolele (cineva a ajuns să le știe/obțină, indiferent cum), schimbă-

¹⁹ UNICEF, Policy guidance on AI for children, 2.0 | NOVEMBER 2021. Disponibil pentru download direct, la:

<https://www.unicef.org/globalinsight/media/2356/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf>

²⁰ Google AI, Making AI helpful for everyone. Disponibil la: <https://atozofai.withgoogle.com/intl/en-US/>

²¹ Sfaturi pentru navigarea sigură pe internet. Disponibil la: <https://www.tirnaveni.ro/sfaturi-pentru-navigarea-sigura-pe-internet/>

acolo sunt foarte importante. Îți vom prezenta doar un scurt rezumat, cu accent pe problemele cu care se confruntă copiii în mediul online.

Unul dintre aspectele pe care realizatorii cercetării și-au propus să le lămurească a fost “Pe care dintre următoarele lucruri știi să le faci pe internet?”, iar rezultatele au arătat că aproape toți elevii intervievați (93%) declară că “știi cum să blocheze o persoană care îi deranjează pe internet (pe rețelele de socializare, e-mail sau aplicație de online messaging)”, însă, acest procent scade atunci când trebuie să facă setări ce presupun să aibă mai multe cunoștințe, cum ar fi: să schimbe “setările de confidențialitate ale profilului de pe rețelele de socializare (79%), blocarea pop-up-urilor cu notificări (66%), verificări privind securitatea site-ului pe care au intrat (63%)”.

Studiul a mai arătat că sub jumătate din elevii cu vârste între 10 și 18 ani (48%) știu să activeze sau să schimbe filtrele, adică “modul în care calculatorul ori browser-ul de internet selectează ce site-uri sau ce conținut pot vedea”.²³

Un alt aspect pe care studiul și-a propus să-l clarifice a fost cel legat de temerile copiilor privind pericolele la care se expun când navighează pe internet. Studiul a scos în evidență faptul că “60% dintre elevii cu vârste cuprinse între 10 și 18 ani susțin că sunt îngrijorați de faptul că ar putea deveni victime ale tuturor infracțiunilor de acest tip enumerate în chestionar”.

Cel mai mare număr dintre elevii participanți la studiu se tem de “furturile de identitate și de spargerea conturilor de pe rețelele de socializare/de e-mail/jocuri online (74% dintre elevi sunt foarte sau destul de îngrijorați)”. Elevii se tem foarte tare și de faptul că “ar putea exista persoane care să le facă avansuri sexuale pe internet, ori că ar putea fi șantajați să facă unele lucruri pentru a nu fi răspândite poze, filmulețe, zvonuri ori divulgate informații despre ei (64% dintre respondenți)”.²⁴

Întrebați dacă, de când utilizează internetul li s-a întâmplat vreodată să fie victima vreuneia dintre situațiile amintite mai sus, destul de mulți elevi au afirmat că au fost victime ale diverselor tipuri de infracțiuni pe internet. Mai bine de o treime dintre ei (39%) “au remarcat că au avut dispozitivele pe care le utilizează afectate de softuri malițioase [...] sau au dat, din întâmplare, în timp ce navigau pe internet, de materiale pornografice (38%)”.

Un număr relativ mare de elevi a declarat că “au fost victime ale altor fapte, ceva mai grave (spargerea conturilor de pe rețelele de socializare - 24%, hărțuire - 15%, avansuri sexuale - 11% sau chiar furt de identitate - 11%)”.²⁵

Studiul a mai scos în evidență faptul că “apar destul de des situații în care le sunt solicitate materiale cu caracter pornografic (fotografii, filmulețe cu ei dezbrăcați, în ipostaze intime sau sexuale) - 125 dintre elevii chestionați (9%) au afirmat că li s-au cerut pe internet astfel de materiale” și că “uneori, conversațiile video în care sunt implicați minorii pe internet includ și solicitarea ca aceștia să se dezbrace, astfel încât să fie văzuți de către cealaltă persoană (54% dintre elevii chestionați au afirmat că li s-a solicitat acest lucru)”.²⁶

Elevii participanți la cercetare au mai relatat și faptul că “au existat și situații în care elevilor li s-au solicitat bani în schimbul deblocării/recăștigării controlului asupra propriului dispozitiv ori în schimbul recăpătării accesului la propriul cont de pe rețeaua de socializare, e-mail sau joc online. De asemenea, au fost semnalate de către minori și situații în care au fost șantajați să facă lucruri pe care nu voiau să le facă sau li s-au solicitat sume de bani pentru a nu fi divulgate informații despre ei, sau pentru a nu fi răspândite poze, filmulețe cu ei sau zvonuri despre ei”.²⁷

²³ Ibidem.

²⁴ Ibidem.

²⁵ INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE, Institutul de Cercetare și Prevenire a Criminalității, Riscuri și vulnerabilități ale elevilor în mediul online, RAPORT DE CERCETARE, 2021. Disponibil pentru download direct, la:

https://www.politiaromana.ro/files/pages_files/raport_cercetare_Proiect_Cyberex.pdf

²⁶ Ibidem.

²⁷ Ibidem.

8. Agresiunea de tip cyberbullying se pedepsește?
9. Companiilor prezente online nu pare să le pese de bullying online și de hărțuire. Sunt trase la răspundere?
10. Sunt disponibile instrumente online anti bullying pentru copii sau tineri?

Exemple de cyberbullying

Te rugăm să citești cu atenție cele de mai jos, pentru că îți oferim câteva exemple de situații în care este cyberbullying, fără niciun dubiu³⁰:

- Hărțuirea cuiva prin trimiterea de SMS sau mesaje instant, în număr mare, pentru a amenința sau a intimida destinatarul, sau chiar fără un scop precis, pur și simplu pentru a deranja destinatarul prin multitudinea notificărilor care anunță primirea unui mesaj;
- Farse făcute cuiva, folosind telefonul persoanei respective (lonel trimite Alinei mesaje nepotrivite, de pe telefonul lui Gigel);
- Accesarea, fără permisiune, a profilului de jocuri sau de rețele sociale al altcuiva și utilizarea acestuia pentru a modifica respectivele profiluri, sau pentru a face farse cuiva;
- Jignirea, amenințarea, intimidarea, șantajarea cuiva, indiferent de motiv, în mediul online;
- Divulgarea în mediul online a secretelor încredințate de cineva, sau răspândirea de zvonuri sau de minciuni despre cineva;
- Crearea sau asocierea la un grup (bandă, gașcă) cu scopul de a amenința, intimida, șantaja, jigni, umili, hărțui etc. persoane în mediul online;
- Postarea de texte și/sau imagini/clipuri video despre tine, fără permisiunea ta și, mai ales, adăugarea la acestea de comentarii jignitoare la adresa ta, pentru a te umili și pentru a atrage și pe alții să facă la fel, sau să distribuie și către alte persoane;
- Răspândirea în mediul online a detaliilor tale personale (poze, filme, număr de telefon, adresa de e-mail, adresa unde locuiești, școala/clasa unde înveți, cine sunt rudele tale sau prietenii tăi etc.);
- Grooming - este o practică foarte periculoasă, deoarece poți fi manipulat, prin orice mijloace îți poți imagina, să faci lucruri ilegale (să furi, sau chiar să omori pe cineva), sau să faci lucruri cu care, mai apoi, să poți fi șantajat: să te dezbraci și să te lași fotografiat/filmat, să te prostituezi online etc.);
- Răspândirea în mediul online de mesaje jignitoare, care fac rău, folosind identități false;
- Crearea de pagini web, bloguri, vloguri etc. pentru a evalua jignitor și exagerat pe cineva: spre exemplu, așa ziși influenceri care scriu lucruri neadevărate, sau le exagerează, le răstălmăcesc, le prezintă într-o manieră denigratoare pentru persoana evaluată și devenită țintă;
- Păcălirea cuiva să divulge utilizatorul și parola contului de e-mail și/sau contului de socializare, joc online etc. și utilizarea acestora pentru a face rău proprietarului contului, precum și altora.

II.1.12.2. Furtul de identitate

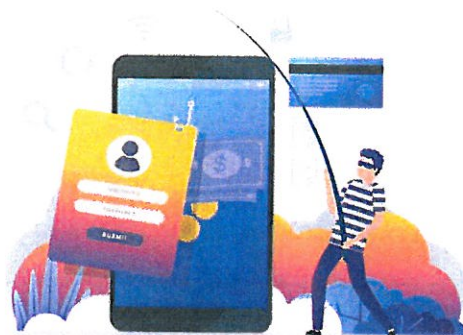
Furtul de identitate are loc atunci când cineva pretinde a fi altcineva pentru a obține bani sau alte lucruri. Azi cerem ajutorul prietenului nostru imaginar, Alex, care ne va ajuta să-ți oferim cel mai bun exemplu ca să poți înțelege cum stă treaba cu furtul de identitate. Alex și-a primit primul card bancar și a fost foarte fericit. Dar, din nefericire, cineva a furat datele cardului său și a început să cumpere lucruri, online, folosindu-i banii.

³⁰ Câteva exemple de cyberbullying. Disponibil la:

<https://www.hockeycanada.ca/en-ca/hockey-programs/safety/cyberbullying/facts/examples-kids-teens-adults>

II.1.12.3.1. Phishing

Criminalul cibernetic „iese la pescuit” pe internet, în speranța că va prinde ceva în cârligul său. Din păcate, are dreptate, pentru că, mereu vor exista victime care vor pica în plasa lui. „Pescarul” nostru pretinde că este o persoană de încredere și, înșelând victima, primește acces la informații sensibile (de exemplu, parole, detalii card bancar). Cel mai mare succes îl are folosindu-se de reclame false și de e-mailuri. În afară de exemplele pe care ți le-am dat mai sus, îți oferim altul, care, din păcate, are, la rândul său o mare rată de succes.



Criminalul cibernetic îți trimite un e-mail, de pe o adresă care pare în regulă, prin care te anunță că ai nu știu ce problemă cu contul bancar personal, cu adresa de e-mail sau cu contul de socializare și trebuie să o rezolvi urgent, altfel pierzi contul, banii, adresa de e-mail etc. Pentru asta, ți se cere să dai click pe un link și să completezi acolo datele care ți se cer. Din momentul în care ai dat click pe acel link, ai devenit victima criminalului cibernetic.

Poți fi păcălit și prin telefon, de o persoană care pretinde că sună din partea unei surse de încredere (banca ta, un membru al familiei, o autoritate oarecare, cineva de la școală) care îți solicită informații confidențiale, cum sunt adresa, nume complet, datele părinților etc.

Cum te afectează?

- Pierzi date personale generale și date sensibile;
- Pierzi accesul la conturi (e.g. e-mail, rețele de socializare etc.);
- Pierzi date financiare;
- Instalezi malware (virusi) și alte amenințări informatice;
- Poți infecta și alte dispozitive din rețea;
- Devii sursa atacurilor care vizează prieteni, instituții, organizații etc.

Cum îți dai seama că poți fi victima unui atac de tip phishing?

- Ți se atrage atenția și ești îndemnat să faci ceva **URGENT!**, cum ar fi să schimbi parole, să pui o adresă de e-mail alternativă pentru recuperarea celei de bază, și ți se da o adresă care ți se cere să o folosești, să actualizezi datele personale etc.). Noi te asigurăm că **NIMIC** nu este atât de urgent. Înainte de a face ce ți se cere, solicită ajutorul unui adult de încredere;
- Se solicită introducerea de date confidențiale folosind un link către un site indicat în textul mesajului sau deschiderea unui fișier atașat, care este infectat și tu nu știi. Iarăși, **NIMIC** nu trebuie făcut atunci. **NICIODATĂ** nu-ți va cere banca ta de încredere, spre exemplu, să faci asemenea lucruri;
- Mesajele conțin erori gramaticale (atacatorii nu sunt întotdeauna români și folosesc, spre exemplu, Google translate sau alte instrumente pentru a traduce text în limba română, ceea ce generează destule erori de exprimare, dezacorduri gramaticale etc.; nu e cazul să râzi de ei că-s analfabeți și să faci ce-ți cer, pentru că, în cazul acela, rămâi **TU** „repetent” la măsuri de protecție și riști să pierzi tot; atunci, cine râde mai cu folos, dintre voi doi?);
- Ofertele care sunt prea bune pentru a fi adevărate. Chiar te crezi atât de norocos încât să primești gratuit un telefon ultimul răcnet, dacă **TOT** ce trebuie să faci este să dai click pe un link și, eventual, să dai ceva date, dar nu trebuie să plătești nimic, sau o sumă derizorie?;
- Chiar crezi că salvezi, cu un simplu click, viața cățelușei Puffy, care e atât de dragălașă în videoclipul pe care ai fost îndemnat să-l vezi și care are nevoie urgent de o operație chirurgicală? Cere imediat ajutorul unui adult de încredere, care să te ajute să-ți cureți calculatorul de „balauri”.

În Evul Mediu erau des întâlnite epidemiile de ciumă, o boală contagioasă, încă neeradicată!, determinată de *Yersinia pestis*, o bacterie transmisă la om prin mușcătura de purice. În cazuri rare, extinderea infecției bacteriene la nivel pulmonar poate determina răspândirea interumană prin intermediul secrețiilor contaminate³⁴.

În Europa, ciuma a fost adusă tocmai de aceste corăbii, pline de rozătoare purtătoare de boală, dar și de purici, odată cu marinarii și pasagerii ce se aflau pe ele.

În analogia noastră, Stick-ul USB media este corabia plină de mărfuri, dar, potențial, și de „agenți patogeni”, în cazul nostru, tot felul de viruși și alte programele care abia așteaptă să pună stăpânire pe dispozitivele tale. Stick-ul USB media a devenit atât de comun în utilizarea noastră, încât nu mai realizăm că ar putea fi purtător și transmitător de viruși, mai ales că îl introducem cu atâta ușurință în tot felul de dispozitive pe care nu ne mai obosim să le verificăm dacă nu sunt infectate și ne-ar putea „îmbolnăvi” și dispozitivul nostru.

Apare, însă, firească întrebarea: Cum ne protejăm de virușii informatici în acest caz?

Toate precauțiile pe care știi că trebuie să le iei pentru a proteja un computer, se aplică, identic și pentru Stick-ul USB media, cum ar fi: scanarea Stick-ului USB media cu programe antivirus, nu copiem pe el fișiere cu proveniență nesigură, aplicăm principiul „Zero Încredere”, adică nu permitem nimănui acces la dispozitivul nostru.

II.1.12.3.3. Social Engineering (inginerie socială)

Toți cunoaștem povestea Capra cu trei iezi. După cum știm, lupul își schimbă vocea, cu scopul de a-i păcăli pe iezi ca să-i deschidă ușa. Lupul face în așa fel încât să imite vocea mamei, deci, a cuiva cunoscut în care copiii au încredere. Tot la fel, atacatorii cibernetici caută să vă câștige încrederea prin folosirea în comunicare a unor elemente familiare, foarte bine cunoscute vouă. Cu cât elementul comun cunoscut este mai special și mai deosebit, cu atât veți spune că este cineva cunoscut care vă solicită pe internet informații ce par inofensive. Deschiderea ușii de către iezi din poveste, după ce au fost păcăliți de lup, este echivalentă cu apăsarea unei taste de pe telefon la solicitarea mincinoasă a cyberlupului.

Cum poate cyberlupul să te păcălească?

Îți oferim mai departe câteva exemple cât se poate de plauzibile:

- Ți se adresează pe nume, pentru a crea aparența prieteniei și a familiarității;
- Face un comentariu pozitiv sau de susținere față de o situație pe care ai postat-o pe o rețea de socializare, pentru a-ți capta atenția și a-ți câștiga simpatia și încrederea;
- Îți spune că vorbește în numele unuia dintre părinți, a unei rude sau al unui prieten, care nu e disponibil la momentul vorbirii și care este într-un mare pericol, astfel încât doar informația pe care ți-o va solicita cyberlupul va constitui salvarea de la pericolul iminent în care se află aceștia;
- Privește peste umărul tău, fără să-ți dai seama și observă parola, codul pin etc.
- Te roagă să-i împrumuți telefonul pentru un apel urgent (ceva de viață și de moarte);

Ingineria socială este o strategie utilizată de indivizi, sau de grupuri, pentru a manipula oamenii și a-i induce în eroare în vederea dezvăluirii unor informații sensibile sau efectuării de acțiuni



³⁴ Medcover, Ciuma - o boala infecțioasă care încă nu a fost eradicată. Disponibil la:

<https://www.medcover.ro/despre-sanatate/ciuma-o-boala-infectioasa-care-inca-nu-a-fost-eradicata,1033,n,295>

- **Protejează-ți parolele!** Dacă altcineva îți cunoaște parola, ți-o poate schimba și poate să-ți interzică accesul la contul tău. De asemenea, se poate preface că ești tu și poate vorbi în numele tău, îți poate strica rankingul la jocuri, îți poate distribui fotografiile și poate distribui informații false. Chiar dacă ai cea mai corectă și puternică parolă, nu mai valorează nimic dacă o spui altora.

Nu oferi niciodată parola, nici măcar celor mai buni prieteni ai tăi - nu știi niciodată, cu adevărat, ce s-ar putea întâmpla cu ea sau cu informațiile tale! Nu folosi ca parolă numele pisicii, al câțelului sau al tău! A avea o parolă este ca și cum ai avea o cheie de la o ușă. Dacă ușa este încuiată, cheia îți permite să o deschii. O parolă este o cheie digitală care oferă acces la dispozitivul tău, sau la ceva instalat pe acesta, sau la o aplicație online. Este important să îți protejezi informațiile cu parole puternice, care sunt ușor de reținut pentru tine, dar greu de ghicit pentru altcineva.³⁸

- Gândește-te de două ori înainte să dai click pe link-uri sau când descarci fișiere! Ar putea fi viruși deghizați sau trimiși de cineva care vrea să-ți fure datele personale.
- Dacă ai propriul tău cont de e-mail, anunță-ți părinții dacă primești vreodată un e-mail prin care cineva (mai ales cineva necunoscut) îți solicită informații personale. Unele e-mail-uri par oficiale, de parcă ar fi fost trimise de la școală, dar ar putea fi un truc pentru a obține datele tale personale.
- E-mail-urile false conțin, de multe ori, cuvântul "urgent", asociat cu un îndemn la o acțiune: "Dă click aici și actualizează-ți urgent datele contului, altfel se va închide mâine!", "Contul tău [de] a fost spart și trebuie să schimbi urgent parola. Dă click aici!"
- Când îți scrie o persoană necunoscută, spune-le părinților tăi sau altor adulți în care ai încredere, în mod special atunci când îți cere să vă întâlniți. Dacă persoanele necunoscute îți scriu pe chat, cel mai bine este să le ignori. Nu poți ști niciodată cine sunt în viața reală.
- Nu intra în concursuri online, nu te alătura unor cluburi/caste/ghilde/triburi/familii etc., folosind datele tale personale (nu folosi numele tău real sau orice alte informații care ar putea să le folosească altora să-ți facă rău). Dacă vrei să participi la un concurs online și trebuie să furnizezi informații personale pentru înscriere, participare și, eventual, premiere, roagă-ți părinții sau profesorii să verifice înainte dacă totul este în regulă.
- Dacă o ofertă la orice te-ar putea interesa ți se pare prea bună pentru a fi adevărată (cel mai adesea, prea ieftină sau chiar gratuită), atunci probabil că este falsă. Sigur ai primit oferte prin e-mail care îți ofereau ceva gratuit, cum ar fi un telefon mobil sau bilete la concert, nu-i așa? Acestea pot fi trucuri menite să te facă să renunți și să dai date personale, sau să dai click pe linkuri pentru a instala diverse extensii sau aplicații fără de care ți se spune că nu poți primi acele produse, dar, de fapt, riscă să-ți introducă automat malware sau spyware în dispozitiv.
- Când ai dubii despre ce se petrece în mediul online, ceva te deranjează sau ți se pare nepotrivit, vorbește cu părinții tăi sau alți adulți în care ai încredere. Dacă cineva te necăjește online, spune-le părinților tăi!³⁹



³⁸ Zuky The Robot, *Complex Passwords*. Disponibil la:

https://www.youtube.com/watch?v=PeG_WRV9iQM&list=PLZ11jQtA2fL11yY06-HnpsrJifRsYoeFg

³⁹ International Association of Privacy Professionals - IAPP, *Safe Space: A Kids Guide to Data Privacy*. Disponibil la:

<https://iapp.org/resources/article/safe-space-a-kids-guide-to-data-privacy/>

- Ai dreptul la justiție. Statul trebuie să se asigure că sistemul de justiție este adaptat drepturilor și nevoilor tale specifice.

Libertățile tale

- Libertatea de opinie: de îndată ce ai această capacitate, ai dreptul să-ți exprimi opinia cu privire la orice te privește. Opinia ta trebuie luată în considerare.
- Libertatea de expresie: ai dreptul să te exprimi liber și să cauți, să primești și să diseminezi informații.
- Libertatea de gândire, de conștiință și de religie.⁴⁰

Potrivit Legii nr. 272/2004, copiii au dreptul la libertate de exprimare și trebuie să aibă posibilitatea neîntărită de a căuta, de a primi și de a transmite informații de orice natură, care vizează promovarea bunăstării lor sociale, sănătatea lor fizică și mentală.

Părinții și ceilalți responsabili legali ai copiilor, precum și orice alte persoane care au obligația de a asigura respectarea drepturilor lor, trebuie să le dea informațiile, explicațiile și sfaturile necesare, în funcție de vârstă și de capacitatea acestora de a înțelege la momentul respectiv. În orice caz, aceștia au obligația de a-i lăsa pe copii să-și spună punctul de vedere, să-și prezinte ideile și opiniile așa cum consideră.⁴¹

Tot în acest sens sunt și prevederile Convenției ONU cu privire la drepturile copilului, potrivit căreia: „Copilul are dreptul la libertatea de exprimare; acest drept cuprinde libertatea de a căuta, de a primi și de a difuza informații și idei de orice natură, indiferent de frontiere, sub formă orală, scrisă, tipărită sau artistică ori prin orice alte mijloace, la alegerea copilului”⁴².

⁴⁰ COUNCIL OF EUROPE, Children's Rights. Disponibil la:

[https://www.coe.int/en/web/children/i-have-rights-you-have-rights-he/she-has-rights-...#%2212444981%22:\[1\]}](https://www.coe.int/en/web/children/i-have-rights-you-have-rights-he/she-has-rights-...#%2212444981%22:[1]})

⁴¹ Voiculescu Simona, Redactor-șef, avocatnet.ro, Libertatea de exprimare a copiilor este doar unul dintre drepturile „uite” ale acestora. Disponibil la:

https://www.avocatnet.ro/articol_44911/Libertatea-de-exprimare-a-copilor-este-doar-unul-dintre-drepturile-%E2%80%99Euitate-ale-acestora.html

⁴² CONVENȚIE cu privire la drepturile copilului, adoptată de Adunarea Generală a Organizației Națiunilor Unite la 20 noiembrie 1989. Disponibil la: http://www.cdep.ro/pls/legis/legis_pck.http_act_text?id=28213

III. PĂRINȚII

Beneficiile lumii online depășesc cu mult dezavantajele acesteia. Copiii trebuie să știe cum să navigheze pe internet pentru a fi productivi și competitivi în viitor, deoarece lumea digitală este a lor și în ea își vor trăi viața. Cu toate acestea, copiii sunt foarte impresionabili și s-ar putea să nu fie pregătiți pentru tot ce se găsește pe internet.

Curiozitatea lor naturală, combinată cu lipsa lor de maturitate, îi poate face să răătăcească în zone cibernetice nesigure. Conținutul neadecvat pentru vârsta lor rămâne cel mai mare risc pentru ei. Învățarea copiilor despre siguranța și confidențialitatea online ar trebui să înceapă cu dvs., părinții și profesorii lor. Sunteți adulții în care copiii/elevii voștri au cea mai mare încredere.



Să fii părinte în ziua de astăzi implică creșterea primei generații de copii care cresc înconjurați de tehnologie - la școală sau acasă, sau cu tehnologia devenită aproape o extensie a corpului lor - copii cu telefonul în mână, permanent, nu mai este ceva ce putem vedea ca simbol al unui nivel de trai ridicat (părinți cu o stare materială bună sau foarte bună și care oferă copiilor lor tot ce este mai nou și mai scump în materie de tehnologie), ci este o imagine atât de comună, încât, abia dacă NU vedem un copil cu un telefon de ultimă generație în mână, cu ochii nedezlipiți de ecran nici măcar atunci când trece strada, ni se pare ceva ciudat și aproape nefiresc.

Așa că, înțelegem dorința părinților de a asigura siguranța online a copiilor. Dar, odată cu apariția dispozitivelor mobile, din ce în ce mai complexe, și a noilor platforme de comunicare, adulții au multe de învățat pentru a ține pasul cu vremurile. Acest ghid oferă sfaturi practice despre cum, când și de ce să vă ajutați copiii să se bucure în siguranță pe internet și de tot ceea ce acesta are de oferit.

III.1. Ce trebuie să știe părinții?

Ca părinți, tutori, reprezentanți legali ai copiilor cu vârsta sub 16 ani, trebuie să știți că este nevoie de acordul vostru pentru ca acesta să poată accesa servicii ale societății informaționale, adică, un copil cu vârsta sub 16 ani nu ar trebui să poată să instaleze aplicații sau să-și creeze conturi pe rețelele de socializare fără acordul vostru. Fiți vigilenți, deoarece copiii, în dorința lor de independență și în lipsa lor de răbdare să aștepte să treacă anii, până la majorat, exagerează cu privire la vârsta lor și își creează singuri conturi, fără să vă spună. "Minciunica" despre vârsta lor ar putea fi cea mai mică problemă a unui părinte în această situație.

Cele mai mari riscuri și probleme pot apărea DUPĂ ce copilul și-a creat respectivul cont (pe un site de jocuri, pe rețele de socializare etc.), adică există riscul ca fiul/fiica lor, copilul pe care-l au în îngrijire să furnizeze date personale fără discernământ și să adopte o sumă de comportamente periculoase, fără să fie conștienți că se expun, convinși fiind că sunt protejați de anonim, spre exemplu ("Nu mă cunoaște nimeni aici, pot face orice/Nu are cum să-mi facă rău cineva, pentru că nu știe nimeni cine sunt"). Cine vrea cu adevărat să-i păcălească pe copii și să profite de pe urma lor, va găsi întotdeauna metoda potrivită să o facă.

În general, răufăcătorii cibernetici încearcă să vă inducă în eroare copilul și să primească acces la datele sale personale, sau chiar și ale dvs. și/sau ale altor membri ai familiei, în special pentru câștig material, adică pur și simplu fac rost de marfă de vânzare pentru cumpărătorul potrivit (spre exemplu, companii de marketing care cumpără date pentru a crea reclame țintite).

securizată a mediului online, care pot bloca, automat, conținutul dăunător, pot înregistra activitatea copiilor și pot informa părinții cu privire la potențialele “puncte moarte” ale confidențialității datelor. Având în vedere faptul că nicio soluție nu rezolvă complet și în mod absolut sau satisfăcător o problemă, singurul lucru realist pe care îl puteți face este să vă protejați copiii cât mai bine, conștienți fiind că nu o veți putea face nici complet și nici mereu (“Dacă vrei să te ferești de o primejdie, cunoaște-o cât mai bine!”).

Făcând cel mai bun compromis între ce ar trebui să faceți pentru a vă proteja copiii în mediul online și ceea ce puteți face cu adevărat, creați premisele asigurării celei mai bune protecții posibile pentru datele copiilor în mediul online.

III.2. Cine ar trebui să le vorbească copiilor despre datele lor personale și securizarea acestora?

Primii care ar trebui să poarte această discuție cu copiii sunt părinții.

Iată de ce: copiii sunt înconjurați de mulți oameni care joacă roluri foarte importante în viața lor, cum ar fi rude, prieteni și profesori. Cu toate acestea, copiii tind să caute răspunsuri la părinții lor, așa că fiți prezenți și pregătiți pentru a oferi îndrumări și sfaturi. Când ar trebui să vorbiți cu ei despre mediul online și comportamentele responsabile în acest context? Acum! Din prima clipă în care un copil manifestă interes pentru tableta, smartphone-ul sau computerul dvs., ar trebui să începeți să le explicați cum stau lucrurile. Rețineți, așa cum copiii au nevoie de reguli pentru a trăi în siguranță în lumea reală, așa au nevoie de îndrumare și pentru traiul sigur, în lumea online.



În timp ce amenințările imediate la adresa siguranței personale pot veni într-o formă diferită (orice interacțiune fizică, nemijlocită, cu lumea reală, se poate transforma într-o vătămare fizică sau psihică), potențialul de vătămare în mediul online este la fel de real (o răpire, sau alt tip de vătămare fizică, cât se poate de concretă în viața reală, își poate avea rădăcinile în mediul online, ca urmare a unei încrederi prost plasate a copilului în cei cu care intră în contact acolo).

Pe măsură ce copilul crește, în calea lui apar noi provocări în interacțiunea sa cu mediul. Îndrumarea părinților va ajuta copiii să ia decizii cât mai bune și să aibă un comportament responsabil, pentru propria siguranță, dar și în relația cu ceilalți (copiii nu trebuie să învețe doar cum să se protejeze pe ei înșiși, ci pot contribui și la educarea altora și, deloc lipsit de importanță, pot învăța, spre exemplu, că cyberbullying-ul este interzis nu doar când efectele acestuia se manifestă direct asupra lor, ci este un comportament interzis și lor, adică nici copiilor dvs. nu le este permisă această practică).

Trăiți acut sentimentul că fiii și fiicele dvs. știu mai multe despre tehnologie și digitalizare decât știți voi? Este un sentiment real și cât se poate de justificat. Copiii din zilele noastre sunt nativi digitali⁴⁴, care, în termeni extrem de simpli, sunt foarte abili în utilizarea noilor tehnologii. Cu

⁴⁴ ECDL Foundation 2014, *Eroarea “Nativ Digital”*: De ce tinerii trebuie să își dezvolte competențe digitale: Termenul “nativ digital” a fost inventat în anul 2001 de către autorul american Marc Prensky. În articolul său, “Digital Natives, Digital Immigrants”, Prensky a definit nativii digitali ca fiind tinerii ce au crescut înconjurați de și folosind computerele, telefoanele mobile și alte instrumente ale erei digitale. Autorul a susținut că un mediu digital schimbă dramatic felul în care oamenii gândesc și procesează informația - este posibil chiar să le modifice structura cerebrală. Prensky a comparat nativii digitali cu imigranții digitali, definiți ca cei care s-au născut înainte de extinderea largă a utilizării tehnologiei digitale și care au adoptat-o într-o anumită măsură mai târziu, pe parcursul vieții. Potrivit lui Prensky, în Statele Unite ale Americii, toți oamenii născuți după 1980 sunt nativi digitali. În anii care au urmat, Prensky a revizuit abordarea sa referitoare la nativii digitali prin adăugarea unui nou concept, “înțelepciune digitală” (“digital wisdom”). Disponibil pentru download direct, la:

https://www.ecdl.ro/uploads/stiri/resources/files/E%5C9Fecul_Genera%C5%A3iei_Nativilor_Digitali_Document_de_pozitie.pdf

supravegherea numărului de ore petrecute de copii online și stabilirea intervalului orar în care le permiteți să desfășoare activități online!

- **Fiți un exemplu bun!**

Copiii tind să urmeze comportamentele părinților. Dacă le demonstrați cum navigați online în siguranță și cum interacționați corect cu ceilalți, este posibil ca aceștia să vă urmeze exemplul. Vă puteți verifica cunoștințele în privința siguranței online făcând diferite teste disponibile pe diverse site-uri, cum ar fi www.sigurantaonline.ro.⁴⁷

Între 11 și 14 ani

- **Învățați-i să nu împărtășească informații care i-ar putea identifica!**

Este foarte important să-i învățați pe copii că, în lumea virtuală, **nu toți sunt prieteni și nu toți sunt cine pretind că sunt**. Explicați copiilor de ce nu este sigur să partajați informații online, cum ar fi adresa de domiciliu sau cea de e-mail, numărul de telefon, detaliile școlii sau programul zilnic. Rugați copilul să vă solicite acordul înainte de a partaja fotografii potențial sensibile. Copiii trebuie să înțeleagă că, odată ce au distribuit ceva online, acel **“ceva”** rămâne acolo și nu mai poate fi șters definitiv niciodată.

- **Mențineți deschis dialogul cu copilul!**

Încurajați copiii să fie deschiși cu dvs. și să întrebe liber despre ceea ce văd pe internet! Încercați să răspundeți întrebărilor despre **„știri false”** sau despre fotografiile false, vorbindu-le despre utilizarea paginilor web/surselor de informații de încredere!

Între 15 și 18 ani

- **Nimeni altcineva nu ar trebui să le cunoască parolele.**

Știm că adolescenții au tendința de a se comporta ca și cum le-ar ști pe toate, dar asigurați-vă că înțeleg și aplică cele mai bune practici atunci când vine vorba de parole. Subliniați că **nu ar trebui să-și împărtășească niciodată parolele cu alte persoane**. Explicați-le de ce parolele nu ar trebui partajate/dezvăluite nici măcar prietenilor, deoarece pot cădea cu ușurință în mâini greșite și ar putea permite accesul la conturile de rețele sociale sau la informațiile bancare.

- **Raportați imediat urmărirea și hărțuirea cibernetică!**

Vă amintiți de agresorul școlii? În zilele noastre, mulți **“bătăuși”** au trecut la tehnologia modernă și se ascund în spatele anonimatului oferit de internet. Ceea ce nu s-a schimbat este faptul că ei încearcă să le facă rău psihologic (sau chiar fizic) altora. Adolescenții ar trebui încurajați să își informeze părinții sau alți adulți responsabili de ei și să salveze, ca probe, orice e-mail-uri, postări sau fotografii legate de hărțuire sau de o atenție nedorită acordată acestora.

- **Tranzacțiile financiare online trebuie să fie sigure**

Achiziționarea de produse și servicii online poate fi perfect sigură - cât timp sunt în vigoare (active) măsuri de siguranță. Până când copiii înțeleg măsurile de siguranță necesare atunci când furnizează informații financiare personale, ar trebui să facă acest lucru doar sub supraveghere.

III.4. Copiii și rețelele sociale

Vă amintiți de vremurile când copiii se jucau în aer liber și veneau acasă doar când le era foame? Internetul a schimbat totul. În zilele noastre, tinerii pot petrece ore întregi, în fiecare zi, pe rețelele sociale precum Instagram, Snapchat, TikTok, WhatsApp, Facebook și Telegram.

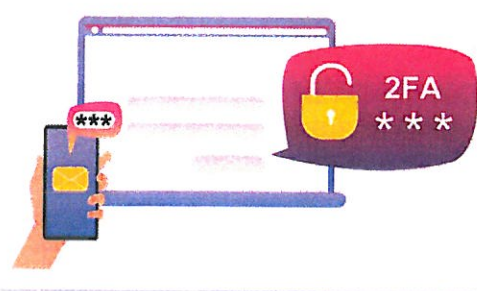
Mulți dintre noi, cei de la ASCPD, suntem părinți, așa că înțelegem de ce s-ar putea să vă îngrijoreze universul online. Am realizat acest ghid strângând informații relevante despre **protecția datelor** și despre **securitatea cibernetică** (sau securitatea online), pentru a vă

⁴⁷ Siguranța online. Disponibil la: <https://sigurantaonline.ro/?fbclid=IwAR1UCwlo8DlaHfgzTDtyklb2AIWdtvNpVB2PYrvrFQj6zj8ieRUERSRmuzo>

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, cu membrii familiei sau cu profesorii.

- **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 agrezeze 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 roțiță dințată). Selectați “Confidențialitate și securitate”, apoi “Confidențialitatea contului”, după care activați “Contul privat”.

- **Câteva recomandări pentru utilizarea în siguranță a rețelelor sociale**

1. 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.
2. 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.
3. 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.
4. Învățați copilul 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.
5. 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.
6. Învățați copilul ca, în cadrul unei rețele de socializare online, precum hi5 sau Facebook, să nu accepte vreodată cereri de prietenie de la persoane pe care nu le cunoaște în viața reală, decât dacă acestea i-au fost recomandate de părinți sau prieteni de încredere.
7. Învățați copilul 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.

Acest comportament ostil este îndreptat, de obicei, împotriva copiilor și adolescenților, deși victime pot fi și adulții. Ținta este amenințată și umilită în spațiul cibernetic de cunoscuții săi, sau chiar de persoane necunoscute. Acest lucru poate provoca traume emoționale extreme sau chiar poate determina victimele să se rănească singure. Cyberbullying-ul se manifestă pe multe căi fiind folosite chiar și funcțiile de chat din cadrul jocurilor din consolă. Subliniați copiilor de toate vârstele că orice formă de hărțuire este inacceptabilă și ar trebui raportată imediat. În plus, în cazul în care copilul dvs. este victimă a agresiunii cibernetice, acesta nu ar trebui să riposteze. Explicați că agresorul dorește să provoace o reacție, oricare ar fi aceasta, deoarece îi alimentează dorința de a face rău altora. Dacă atacurile online continuă, notificați autoritățile competente - oficialii școlii sau forțele de ordine. Nu ștergeți niciun mesaj primit, deoarece ar putea fi folosit ca dovadă.

Grooming

Grooming-ul are loc atunci când un adult încearcă să convingă un copil să presteze activități sexuale fie online, fie în persoană. Un groomer este cineva care construiește o relație de încredere și o conexiune emoțională cu un copil sau un tânăr, astfel încât să îl poată manipula, exploata și abuza, cel mai adesea „împrietenindu-se” pe rețelele sociale. Adesea, un adult se va preface că este un alt copil pentru a stabili o relație de prietenie, apoi încearcă să aranjeze o întâlnire fizică, în viața reală. Pe lângă faptul că ar trebui să țineți evidența cu cine petrec timpul copiii online, reamintiți-le să nu se întâlnească niciodată cu cineva pe care l-au cunoscut online, cu excepția cazului în care un părinte este prezent.



Sexting

„Sexting” (din „sex” și „texting”) există de ani de zile. Deși a apărut cu funcția SMS a telefoanelor mobile, acum pot fi trimise, cu ușurință, mesaje text, fotografii și videoclipuri cu caracter sexual explicit. Amintiți-le copiilor că, odată ce au distribuit astfel de materiale online, acestea se pot răspândi necontrolat. Fotografiile pot fi folosite pentru șantaj, hărțuire cibernetică și multe altele. O regulă de bază este să nu partajați nimic din ce nu ați dori să fie postat public.

Furtul de date și de identitate

Informațiile trimise prin internet, fără a fi luate măsurile de precauție necesare (criptarea datelor sau utilizarea unui site web securizat), pot fi interceptate de terți. În cazul numerelor de cont și a informațiilor bancare, a codurilor numerice personale etc., acestea pot fi apoi utilizate pentru accesarea conturilor bancare și, implicit, pentru furtul banilor din cont sau pentru furtul identității. Asigurați-vă că se cunoaște faptul că organizațiile de încredere și cu reputație nu vor solicita copiilor, prin e-mail sau chat, datele contului sau numerele PIN bancare.

III.6. Cum pot contribui la securitatea digitală a copilului meu?

Să începem cu câteva întrebări pe care, poate, vi le-ați pus deja sau începeți acum:

1. Aveți stabilite regulile casei pentru utilizarea tehnologiei?
2. Aveți stabilite reguli pentru siguranța copilului în lumea fizică?
3. V-ați confruntat cu amenințări din lumea digitală?
4. Există, acasă, o regulă pentru timpul petrecut pe internet?
5. Utilizați controlul parental pe anumite dispozitive (TV, computer, laptop, tabletă, telefon)?
Pe care anume?

- Ce îți place să faci pe laptop/ (iPod/tabletă etc.)?
- Pot să mă alătur și eu?
- Ce site-uri îți place să vizitezi?
- Care sunt personajele tale preferate? (Copiii se uită adesea la televiziune online).
- Pe ce site-uri web sau jocuri crezi că petreci cel mai mult timp?
- Care este activitatea ta preferată în online?



Este important să aveți cunoștință despre momentele în care copilul dvs. joacă jocuri online cu persoane pe care nu le cunoașteți. Rugați-l să vă învețe cum funcționează, cum se joacă jocul respectiv. Fiți entuziasmat și implicat (sau cel puțin arătați un interes real, astfel încât să fie bucuros să vă împărtășească experiența sa).

- Ce îmi poți spune (despre jocul pe care îl jucați/aplicația pe care o utilizați)?
- Cu cine te joci? Poți să vorbești cu ei în joc? Care e numele lor? Cum ați devenit prieteni?

Puneți întrebări specifice, dacă sunteți îngrijorat:

- Ai nelămuriri, vrei să mă întrebi ceva?
- Te supără, te îngrijorează anumite lucruri care s-au petrecut în online? Este în regulă dacă faci o greșală, poți să îmi spui. Te pot ajuta să rezolvi asta. Trebuie să-mi spui dacă cineva nu este drăguț cu tine sau cu unul dintre prietenii tăi în online.
- Putem vorbi despre orice se întâmplă în online, sunt aici ca să te ajut să te distrezi și să înveți! Acasă este un loc sigur. Vom rezolva împreună orice problemă.

Faceți din comunicarea despre tehnologie și internet o parte normală a vieții dvs. Îndrumați-i în deciziile lor, acum, când sunt copii, pentru a-și crea obiceiuri bune pentru viitor!

Copilul vă poate transmite semnale - fiți gata să le recunoașteți!

Căutați/observați semne de:

- dependență de calculator sau telefon ("Majoritatea timpului este petrecut pe calculator/telefon, stare de irascibilitate și comportament agresiv în absența internetului, tulburări ale somnului, neglijarea regimului alimentar sau a igienei personale, îndatoririle școlare nu mai sunt atât de importante pentru el");⁵²
- agresiune (în limbaj sau chiar fizică);
- anxietate (generată de lipsa "drogului").

Vă cunoașteți copilul mai bine ca oricine altcineva. Observați dacă:

- Manifestă agresivitate crescută, în special imediat după utilizarea tehnologiei;
- Manifestă frustrare, în special pentru faptul că nu poate utiliza tehnologia;
- Exprimă îngrijorare pentru că tocmai a părăsit jocul pe care l-a jucat și nerăbdare de a relua jocul, cât mai curând (vorbește despre joc și când nu este în joc);
- Ascunde adevărul în legătură cu timpul dedicat jocurilor;
- Evită contactul cu cei din jur sau se izolează pentru a utiliza internetul.

Ce alte indicii ați putea primi, pentru a descoperi că ceva nu este în regulă?

⁵² Wind Discovery, *Cum să-ți "tratezi" copilul de dependență de internet*. Disponibil la:

<https://www.winddiscovery.ro/blog/tratare-dependenta-calculator/>



AVERTIZARE! Filtrarea conținutului sau monitorizarea dispozitivelor nu ar trebui să fie niciodată invocate ca un panaceu sau ca un înlocuitor pentru supravegherea parentală uzuală ("Copilul meu are nevoie și de mine, nu numai de monitorizarea digitală").

III.8. Recomandări pentru părinți

Evident, interzicerea accesului copiilor la tehnologiile online nu este o opțiune. Dispozitivele digitale fac parte din viața lor de zi cu zi și sunt din ce în ce mai importante pentru dezvoltarea lor. Ajutați-vă copiii să le folosească în siguranță și luați parte la interacțiunea dintre copil și acel dispozitiv. De asemenea, merită remarcat faptul că multe dintre riscurile de mai sus pot afecta și adulții și că regulile de siguranță pe internet se aplică utilizatorilor de toate vârstele.⁵³

Fiți prezent și implicat!

Încercați să aflați/să știți mereu când, unde și cum folosesc copiii internetul. Arătați interes pentru site-urile pe care le vizitează și pentru jocurile pe care le joacă. Atunci când copiii dvs. sunt pregătiți să aibă un cont pe o platformă de socializare, creați unul împreună cu ei. Plimbați-i prin platformă și ajutați-i să înțeleagă setările de confidențialitate ale acesteia. Oferiți-le sfaturi pentru situațiile când primesc solicitări de prietenie de la persoane din afara cercului lor. Stabiliți limite, comunicați și fiți sincer cu copiii, dar amintiți-vă că sunteți, în primul rând, părintele lor și, nu în ultimul rând, prieten. Copiii trebuie să realizeze că nu pot să-și păstreze activitățile online 100% confidențiale. Asigurați-vă copiii că, doar pentru că sunt verificați din când în când, nu înseamnă că nu aveți încredere în ei.

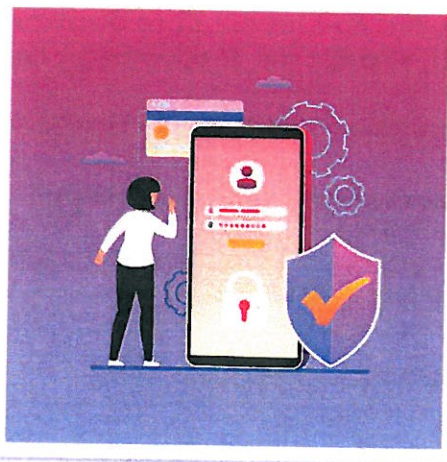
Prețuiți datele personale ale copilului!

În calitate de părinte aveți dreptul să protejați (și, dacă este necesar, să rețineți) detaliile personale despre copiii dvs. Învățați-i să-și protejeze și să prețuiască informațiile personale. Explicați-le de ce ar trebui să vă ceară mai întâi permisiunea, înainte de a furniza în online informații cum ar fi: numele, vârsta, data de naștere și adresa domiciliului lor.

Partajați cu grijă informații despre copii!

Știm că sunteți mândri de copiii dvs., dar, amintiți-vă că postarea de fotografii cu copii creează un traseu permanent, care îi urmărește pe măsură ce cresc. Odată ce postați o fotografie online, pierdeți controlul asupra ei. Poate fi copiată, etichetată, salvată și folosită cu ușurință, în orice scop pe care nu vi l-ați fi imaginat. Tot ceea ce postați conține informații valoroase pentru agențiile de publicitate și pentru colecții de date, dar, și pentru răufăcători (mai ales pedofili).

Verificați setările de confidențialitate!



Fiți atenți la informațiile pe care dvs. și copiii dvs. le partajați atunci când utilizați aplicații online și vizitați pagini web. **Verificați și ajustați setările de confidențialitate** ale dispozitivului, browser-ului, aplicațiilor și conturilor de pe rețelele sociale pe care le utilizați. În cazul în care copilul folosește un smartphone, îl puteți face mai sigur dezactivând serviciile de localizare și împiedicând aplicațiile să partajeze date. Aveți puterea de a decide cine poate să-i vadă postările. Învățați copilul să se comporte ca și cum internetul ar fi un spațiu public, în care "privatul" nu există decât dacă el nu face nimic public. Asigurați-vă că înțelege elementele de bază ale unui

⁵³ ESET, Saferkidsonline, *A safer internet for children - a parents' guide*. Disponibil pentru download direct, la: https://saferkidsonline.eset.com/files/SKO_Safer_internet_for_children_parents_guide.pdf

- Copilul ar trebui să conștientizeze faptul că sunt momente când nu are voie să folosească tehnologia:
 - Trebuie să am ceva timp fără tehnologie, în fiecare seară, înainte de culcare;
 - Nu folosesc niciodată dispozitive conectate la internet în dormitor;
 - Nu există tehnologie permisă în dormitorul meu noaptea, astfel încât să dorm bine;
- Copilul trebuie să fie conștient de importanța confidențialității parolei:
 - Îmi protejerez parolele;
 - Nu împărtășesc parola mea nimănui, cu excepția părinților;
 - Măcar unul dintre părinții mei are parolele mele pentru orice dispozitiv sau site web.

lată câteva resurse care vă pot fi de folos:

Securitate pe internet pentru copii:

- Cyber4Kids. Bun venit la Cyber City!
- Cyber4Kids. Ne jucăm în siguranță
- Cyber4Kids. Date personale secrete
- Cyber4Kids. Cine te păcălește on-line
- Cyber4Kids. Internetul nu uită niciodată
- Cyber4Kids. Cyberbullying
- Cyber4Kids. WiFi sau nu?
- Cyber4Kids. Parole magice

Cinci metode pentru a folosi mai puțin telefonul:

- Cât timp stai în fața ecranului?
- Model de reguli pentru copii
- Model de reguli pentru adolescenți și preadolescenți
- Model de reguli pentru părinți
- Angajamentul privind siguranța pe internet
- Ghid pentru părinți TikTok
- TikTok: sfaturi de siguranță pentru familii
- Ghid pentru părinți, Snapchat
- Ghid pentru părinți, Instagram
- Ghidul familiei pentru controlul parental
- Ghid pentru părinți, Cyberbullying
- Internetul contează, deoarece copiii merită o lume digitală sigură

NOTĂ * Pentru setarea subtitrării în limba română pe <https://www.youtube.com/> alegeți din setări "Subtitles" (subtitrări) și apoi alegeți limba română din listă.

IV. ȘCOALA ȘI PROFESORII

Instrumentele și aplicațiile tehnologice fac posibilă colaborarea între profesori și elevi, pentru a crea și împărtăși idei mai ușor ca oricând. Când școlile folosesc tehnologia în activitatea didactică, datele elevilor, inclusiv unele informații personale, sunt colectate atât de profesori, cât și de companiile care furnizează aplicații și servicii online.

Ca profesori folosiți unele dintre aceste date pentru instruirea propriu-zisă și pentru a vă cunoaște mai bine elevii. Este la fel de important să vă protejați elevii, pe cât de important este să-i ajutați să învețe. Acest ghid este menit să vă ajute să utilizați tehnologia în sala de clasă, protejând, în același timp, confidențialitatea elevilor.⁵⁵



Internetul și digitalizarea au schimbat lumea. Smartphone-urile, aplicațiile și rețelele sociale au introdus schimbări semnificative în modul în care cresc copiii și tinerii. Aceste tehnologii deschid noi orizonturi, neprevăzute anterior dar, introduc și riscuri și amenințări necunoscute generațiilor trecute. În această situație, dumneavoastră, profesorii, vă aflați în prima linie de protecție a elevilor, dar, sunteți adesea lăsați fără materiale sau informații utile. Cu toate acestea, rămâne în sarcina dumneavoastră să transmiteți cunoștințe atât despre lumea digitală, cât și despre lumea reală și să pregătiți elevii pentru o viață sănătoasă în ambele lumi.

IV.1. Școala ca operator de date personale

Conform dispozițiilor Regulamentului European nr. 679/2016 (Regulamentul general privind protecția datelor), „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.⁵⁶

În calitate de operator de date personale școala are anumite responsabilități: să desemneze un responsabil cu protecția datelor, obligație valabilă și pentru școlile private, deoarece prelucrează sistematic un volum mare de date personale, să se asigure de respectarea principiilor privind protecția datelor: legalitate, echitate și transparență, limitarea legată de scopul prelucrării, reducerea la minimum a datelor, exactitate, limitări legate de stocare, integritate și confidențialitate. În plus, operatorul este responsabil de respectarea tuturor acestor principii și să poată demonstra această respectare.

De asemenea, operatorii trebuie să implementeze măsuri tehnice și organizatorice pentru protecția datelor personale prelucrate, să respecte drepturile persoanelor vizate (în cazul școlilor: profesorii și personalul auxiliar, elevii și părinții/tutorii/reprezentanții legali ai acestora).

În mod tradițional, dincolo de datele de identificare personală, datele elevilor constau în informații precum prezența, notele, înregistrările disciplinei și dosarele de sănătate. Accesul la acele date era limitat la profesori sau la personalul auxiliar școlar care avea nevoie de ele pentru a satisface nevoile educaționale și de sănătate ale copilului. Odată cu utilizarea tehnologiei în școli, datele tradiționale sunt acum adesea partajate cu companii care furnizează sisteme de informații pentru elevi, platforme online, aplicații utilizate în procesul de învățare etc.

Noile tehnologii, inclusiv computerele personale, dispozitive mobile, aplicații, site-uri, programe și servicii online - sunt utilizate în sălile de clasă în moduri care generează date noi despre elevi,

⁵⁵ ConnectSafely, Kerry Gallagher, Larry Magid, and Kobie Pruitt, *The Educator's Guide To Student Data Privacy*. Disponibil la: <https://www.connectsafely.org/wp-content/uploads/2016/05/Educators-Guide-Data-.pdf>

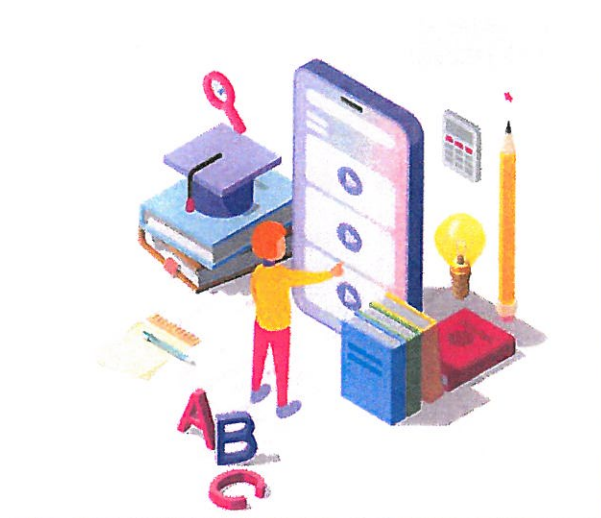
⁵⁶ Regulamentul UE 679/2016. Disponibil pentru download direct, la:

<https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EL>, art. 4, pct. 7

Ce ar trebui să faceți dacă un elev sugerează, pentru un proiect, utilizarea unei aplicații educaționale neverificate?

În calitate de profesor, nu puteți susține oficial utilizarea unui produs extern, dar puteți explica elevului considerentele de care ar trebui să țină seama, inclusiv recomandarea de a-i informa și pe părinți. Este destul de obișnuit ca elevii să găsească singuri aplicații educaționale pe care să le folosească pentru proiecte, iar profesorii ar trebui să încurajeze elevii să fie creativi și să le ia în serios sugestiile. Acesta este un moment de predare - o oportunitate excelentă de a vorbi cu elevul despre confidențialitatea datelor personale și siguranța online.

Iată câteva exemple de întrebări pe care le-ați putea folosi pentru a începe conversația cu elevul dvs.:



1. A trebuit să-ți faci un cont pentru a putea utiliza acea aplicație? Dacă da, a trebuit să furnizezi informații personale (e-mail, nume, vârstă etc.)?
2. Utilizarea aplicației necesită acordul părinților? Cine are acces la emailul tău și la alte informații, acum, după ce ai creat acel cont?
3. Dezvoltatorul aplicației împărtășește datele personale altora? (Ar trebui să găsești astfel de informații în politica de confidențialitate)
4. Aplicația colectează informații suplimentare, cum ar fi locația sau persoanele de contact?

Cel mai probabil, elevul dvs. nu va ști răspunsurile la unele dintre aceste întrebări. Este în regulă, dar este important să-i explicați că toate sunt datele sale personale și trebuie dezvăluite cu precauție. Ar trebui să se gândească la protejarea acestora și ar trebui să fie încurajat să discute despre alegerile sale acasă și cu părinții săi.

Școlilor li se permite să se bazeze pe companiile de tehnologie care furnizează produse și servicii educaționale, dar au responsabilitatea de a se asigura că acești furnizori au implementat măsuri de protecție adecvate pentru datele elevilor. Școala trebuie să se asigure că păstrează controlul direct asupra informațiilor pe care compania le colectează, le utilizează și le menține. Școlile sunt responsabile să se asigure că operatorii care lucrează cu școala, în mod direct utilizează informațiile elevilor numai în scopuri educaționale autorizate. Aceste companii trebuie să aibă acces la aceste date în mod limitat și trebuie să utilizeze informațiile despre elev doar în scopuri educaționale. Școala interacționează cu elevii, pentru toate aceste lucruri, prin dumneavoastră, profesorii.

Ce se întâmplă dacă elevii dvs. și/sau dvs. doriți să utilizați, sau să recomandați un instrument digital care nu a fost conceput special pentru educație?

Dacă dvs., profesorul, doriți să recomandați o aplicație care nu a fost concepută special pentru educație, verificați aplicația cu ajutorul școlii dvs., respectând politicile/procedurile aplicabile. Este o problemă comună, deoarece există multe „aplicații pentru consumatori”, care nu sunt concepute pentru educație, dar pe care elevii ar dori să le folosească pentru a învăța sau pentru a-i ajuta cu temele și cu proiectele lor.

Acestea pot include instrumente de cercetare, aplicații pentru luat notițe, instrumente de colaborare sau aplicații care permit utilizatorilor să realizeze videoclipuri, să înregistreze audio sau să creeze alte produse media, cum ar fi desene animate, imagini și așa mai departe. Cu toate acestea, este posibil ca produsele comerciale care nu sunt concepute și comercializate pentru

le informații despre cum să conlucrați pentru o mai bună siguranță digitală în școli, sau discutând direct cu ei în timpul ședințelor părinți - profesori.

Câteva date care ar trebui să ne dea de gândit:

- Conform [Check Point 2022 Cyber Security Report](#)⁵⁸, educația și cercetarea au fost sectoarele cele mai vizate, organizațiile confruntându-se cu o medie de 1.605 atacuri săptămânale, în anul 2021.
- Atacurile de tip phishing reprezintă peste 80% din atacurile cibernetice raportate.
- Din iulie până în august 2020, Global Threat Activity Tracker de la Microsoft a detectat peste 8 milioane de incidente provocate de malware, educația fiind cel mai afectat domeniu.

Sfaturi de securitate cibernetică pentru profesori:

- Urmați politicile și regulile de securitate cibernetică ale instituției dvs.!
- Folosiți parole puternice!
- Protejați confidențialitatea elevilor!
- Verificați setările platformelor de socializare, în cazul în care aveți un grup pentru elevi sau părinți!
- Verificați setările conturilor dvs. personale de pe rețelele de socializare!
- Utilizați un software antivirus!
- Asigurați securitatea pentru rețeaua Wi-Fi - dacă lucrați de acasă sau predați de la distanță. Alegeți propria parolă pe router, în loc să utilizați acreditările implicite de conectare și schimbați numele routerului atribuit de producător!
- Luați în considerare un produs de tip Virtual Private Network (VPN) - când trimiteți informații printr-o rețea Wi-Fi, o rețea VPN folosește criptarea pentru a vă proteja datele și a le menține în siguranță. Și, deoarece datele dvs. ies de pe serverul VPN, va părea că au adresa de protocol de internet (IP) a acelui server, mascând adresa dvs. IP reală și ascunzându-vă activitatea online.
- Luați în considerare utilizarea Tor Browser - o modalitate de a naviga în mod confidențial pe internet. Utilizarea Tor Browser prezintă numeroase avantaje semnificative din perspectiva securității și confidențialității online. Printre acestea se numără blocarea eficientă a trackerelor care pot urmări activitatea online a utilizatorilor, prevenirea monitorizării istoricului de navigare și ascunderea identității utilizatorului pe internet. De asemenea, Tor Browser oferă criptare multistratificată a datelor, asigurând astfel un nivel ridicat de protecție.

IV.5. Cum să reacționăm la Cyberbullying?

Ce puteți face ca profesori împotriva hărțuirii cibernetice? Părinții și profesorii își pot propune următoarele obiective:

⁵⁸ Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed. Disponibil la: <https://pages.checkpoint.com/cyber-security-report-2022>

Cum să procedați în ceea ce privește sala de clasă în care a avut loc (cyber)bullying-ul:

- Solicitați imediat ajutor în sala de clasă.
- Ajuțați la transformarea experienței negative într-o lecție pe înțelesul elevilor, care explică ce s-a întâmplat, cum este comportamentul specific (cyber)bullying, de ce nu este permis acest lucru și ce poate face sala de clasă pentru remedierea relațiilor interumane.
- Ajuțați elevii în restabilirea sentimentului de siguranță și dezvoltarea de relații sănătoase, folosind activități de grup. Colegii de clasă pot ajuta victima să se simtă mai inclusă și mai sprijinită.
- Implicarea cu succes a elevilor care au participat la rele tratamente în stabilirea relațiilor cu colegii poate fi o modalitate de a împărți responsabilitatea și de a reduce pedeapsa pentru încălcarea regulilor clasei/școlii.
- Puteți recomanda și suport psihologic individual elevilor sau familiilor acestora.⁵⁹



IV.6. Școala și rețelele sociale

Școala și profesorii trebuie să utilizeze mijloace sigure de comunicare cu elevii și părinții. Înainte de a distribui orice informație, să verifice dacă aceasta respectă principiul minimizării datelor, respectiv necesitatea de a divulga acele date către întreaga clasă, sau către/și către întregul colectiv de părinți.

Ne referim aici la distribuirea pe grupuri create pe rețelele de socializare sau pe platforme de comunicare, a listelor cu datele personale ale tuturor copiilor, a notelor/calificativelor acestora, a listelor cu burse școlare sau chiar și a stării de sănătate a copiilor. Astfel de divulgări încalcă prevederile legislației privind protecția datelor personale și pot genera incidente grave de securitate.

Fotografierea copiilor și postarea fotografiilor în mediul online fără acordul părinților încalcă, de asemenea, legislația privind protecția datelor personale.

IV.7. Securizarea datelor cu caracter personal în cadrul educațional

Conform Ghidului Consiliului Europei - Comitetului Consultativ al Convenției pentru protecția persoanelor fizice cu privire la prelucrarea automată a datelor cu caracter personal (CONVENȚIA 108) referitor la Protecția datelor copiilor în cadrul educațional⁶⁰, aplicarea măsurilor de securitate adecvate acestor date și mediilor lor de procesare, atât în repaus, cât și în tranzit, este vitală pentru a ne asigura că datele copiilor sunt protejate la cele mai înalte standarde. Măsurile de securitate ar trebui să țină seama de stadiul actual al tehnicii și metodelor și tehnicilor de securitate a datelor în domeniul prelucrării datelor. Costul acestora ar trebui să fie proporțional cu gravitatea și probabilitatea riscurilor potențiale. Securitatea datelor cuprinde obligații suplimentare, controalele enumerate mai jos sunt deosebit de relevante pentru prelucrare în cadrul setărilor educaționale.

Măsurile de protecție aplicate datelor cu caracter personal ar trebui să se bazeze pe o evaluare a riscurilor, urmând standardele din industrie și cele mai bune practici și folosind îndrumări tehnice stabilite (cum ar fi seria ISO 27000 și altele, după caz).

⁵⁹ ESET, *Digital Security Handbook For Teachers*. Disponibil pentru download direct, la:

<https://saferkidsonline.eset.com/storage/free-downloads/October2021/ISyOqDcONESXDjvx61fW.pdf>

⁶⁰ COUNCIL OF EUROPE, *CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, CONVENTION 108, Children's Data Protection in an Education setting, Guidelines*. Disponibil pentru download direct, la: <https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b>

Trăim într-o perioadă de schimbare constantă care afectează pe toată lumea - familiile, guvernul, afacerile și, bineînțeles, educația. Este o perioadă interesantă și, deși schimbarea rapidă poate fi uneori greu de adaptat, este un fapt al vieții care nu dispăre. În cea mai mare parte, schimbarea este bună, mai ales atunci când ne crește productivitatea și îmbunătățește rezultatele și ajută la implicarea elevilor. Dar, pe măsură ce adoptăm noi tehnologii, trebuie să ne gândim și la modul în care acestea afectează siguranța, securitatea și confidențialitatea tuturor părților interesate, în special a elevilor/copiilor noștri.

Uneori este indicat să facem o pauză, chiar și pentru un moment, pentru a ne asigura că facem tot ce putem pentru a ne proteja elevii și/sau copiii. Dar este și responsabilitatea noastră ca educatori sau părinți să îmbrățișăm inovația și să încurajăm copiii și colegii noștri să încerce noi abordări și să îmbrățișeze noi instrumente. Este o provocare constantă, dar nu este imposibil!

CE FACEM ÎN CAZUL UNUI INCIDENT DE SECURITATE CIBERNETICĂ? RECOMANDĂRILE DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ (DNSC)

NU INTRA ÎN PANICĂ!

În cazul în care ți-a fost compromis contul de pe o platformă de socializare:

Dacă nu mai ai acces la cont:

1. Urmează procedura de recuperare a contului. Dacă nu te descurci singur, contactează centrul de asistență al platformei sociale.
2. Informează furnizorul (platforma socială) despre compromiterea contului.
3. Semnalează fraudă către Directoratul Național de Securitate Cibernetică (DNSC).
4. Informează persoanele din lista de prieteni despre faptul că ți-a fost compromis contul și spune-le să nu acceseze mesaje sau linkuri care le-au fost trimise de pe contul piratat.⁶¹

Dacă ai fost victima unui furt al datelor de card sau al datelor bancare:

1. Ia imediat legătura cu banca emitentă pentru a obține blocarea cardului bancar.
2. Schimbă parolele și aplică autentificarea în doi pași (2FA), acolo unde este posibil.
3. Actualizează software-ul antivirus pentru a fi apărat de orice nou virus informatic și pentru a proteja dispozitivul folosit.
4. Anunță Poliția despre problemă, dacă ți s-au extras bani din cont.
5. Semnalează fraudă către DNSC.
6. Păstrează orice posibilă dovadă a furtului, de exemplu, e-mailuri, facturi, chitanțe, copii ale reclamei etc.
7. Vorbește cu familia și prietenii despre acest incident, ajutându-i, astfel, să fie pregătiți pentru această metodă de atac.⁶²

Dacă ai fost victima unei escrocherii (scam):

1. Ia legătura cu comerciantul, ar putea să existe o altă explicație.
2. Ia legătura cu banca dacă ți-a fost compromis contul bancar și/sau dacă nu îți răspunde comerciantul sau răspunsul său nu este satisfăcător.
3. Schimbă parolele și aplică autentificarea în doi pași (2FA), acolo unde este posibil.

⁶¹ DNSC, *Contul dumneavoastră de pe o platformă de comunicare socială a fost atacat de hackeri?* Disponibil pentru download direct, la: <https://dncs.ro/vezi/document/ce-fac-daca-mi-a-fost-compromis-un-cont-online>

⁶² DNSC, *Ați fost victima unui furt al datelor de card sau de date bancare?* Disponibil pentru download direct, la: <https://dncs.ro/vezi/document/ce-fac-daca-mi-s-au-furat-datele-de-card-sau-de-date-bancare>

BIBLIOGRAFIE

1. 10 sfaturi de protecție online pentru copii și părinți. Disponibil la:
<https://www.descopera.ro/dnews/5489345-10-sfaturi-de-protectie-online-pentru-copii-si-parinti>
2. ARSENE LIVIU, DIRECTOR CERCETARE AMENINȚĂRI INFORMATICE CROWDSTRIKE, "6 PERICOLE LA CARE SE EXPUN COPIII ÎN MEDIUL ONLINE". Disponibil pentru download direct, la:
https://sb.politiaromana.ro/files/news_files/6_Pericole_la_Care_se_Expun_Copiii_in_Mediul_Online_4.pdf
3. Câteva exemple de cyberbullying. Disponibil la:
<https://www.hockeycanada.ca/en-ca/hockey-programs/safety/cyberbullying/facts/examples-kids-teens-adults>
4. certSIGN, "10 trucuri pentru securizarea telefonului mobil". Disponibil la:
<https://www.certsig.ro/ro/10-trucuri-pentru-securizarea-telefonului-mobil/>
5. Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed. Disponibil la:
<https://pages.checkpoint.com/cyber-security-report-2022>
6. Cisco, What is malware? Disponibil la:
<https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html#tabs-35d568e0ff-item-194f491212-tab>
7. ConnectSafely.org, 4 Minutes with TikTok: Safety Advice for Families. Disponibil la:
<https://www.youtube.com/watch?v=m6f8CvRkdh0>
8. ConnectSafely, Children's pledge. Disponibil la:
<https://www.connectsafely.org/child-pledge/>
9. ConnectSafely, FAMILY GUIDE TO Parental Controls, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2021/02/Family-Guide-to-Parental-Controls.pdf>
10. ConnectSafely, FAMILY SMARTPHONE PLEDGE, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2018/05/Smartphone-pledge.pdf>
11. ConnectSafely, INTERNET SAFETY PLEDGE, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2018/05/Parents-pledge.pdf>
12. ConnectSafely, INTERNET SAFETY PLEDGE, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2018/05/Teen-pledge.pdf>
13. ConnectSafely, PARENT'S GUIDE TO Snapchat, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2021/03/Parents-Guide-to-Snapchat-.pdf>
14. ConnectSafely, PARENT'S GUIDE TO TikTok, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2022/05/Parents-Guide-to-TikTok-2022-final.pdf>
15. ConnectSafely, PARENT'S QUICK - GUIDE TO Instagram, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2021/10/Quick-Guide-to-Instagram-2021.pdf>
16. ConnectSafely, QUICK - GUIDE TO Cyberbullying, Disponibil pentru download direct, la:
<https://www.connectsafely.org/wp-content/uploads/2022/04/qg-cyberbullying-2022.pdf>
17. ConnectSafely, Kerry Gallagher, Larry Magid, and Kobie Pruitt, The Educator's Guide To Student Data Privacy. Disponibil la:
<https://www.connectsafely.org/wp-content/uploads/2016/05/Educators-Guide-Data-.pdf>
18. Consiliul European, Consiliul Uniunii Europene, Securitatea cibernetică: ingineria socială. Disponibil la:
<https://www.consilium.europa.eu/ro/policies/cybersecurity/cybersecurity-social-engineering/>
19. CONVENȚIE cu privire la drepturile copilului, adoptată de Adunarea Generală a Organizației Națiunilor Unite la 20 noiembrie 1989. Disponibil la:
http://www.cdep.ro/pls/legis/legis_pck.htm?act_text?idt=28213
20. COUNCIL OF EUROPE, Children's Rights. Disponibil la:
<https://www.coe.int/en/web/children/i-have-rights-you-have-rights-he/she-has-rights-...#%2212444981%22%5B%5D>
21. COUNCIL OF EUROPE, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, CONVENTION 108, Children's Data Protection in an Education setting, Guidelines. Disponibil pentru download direct, la:
<https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b>
22. CURIA, HOTĂRÂREA CURȚII (Camera a treia), 15 septembrie 2016, cauza C-484/14. Disponibil la:
https://curia.europa.eu/juris/document/document_print.jsf?jsessionid=02D734A02B6F26FB4E23F888E5A350C6?docid=183363&text=&doclang=RO&pageIndex=0&cid=1849533
23. Cyber4Kids. Cine te păcălește on-line. Disponibil la:

49. Matthew Sparkes, What does Wi-Fi stand for? Disponibil la:
<https://www.newscientist.com/question/what-does-wi-fi-stand-for/>
50. Medicover, Ciurma - o boala infecțioasă care încă nu a fost eradicată. Disponibil la:
<https://www.medicover.ro/despre-sanatate/ciurma-o-boala-infecioasa-care-incea-nu-a-fost-eradicata,1033,n,295>
51. MelsMine, Ce este furtul de identitate? Disponibil la:
<https://www.furtdeidentitate.ro/furtul-de-identitate/ce-este-furtul-de-identitate/>
52. Regulamentul UE 679/2016. Disponibil la:
<https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=RO>
53. Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică). Disponibil la:
https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.RO&toc=OJ%3AL%3A2019%3A151%3ATOC
54. Screen Time: How Much Is Too Much? Disponibil la:
<https://www.youtube.com/watch?v=fVALeerZpd4>
55. Sfaturi pentru navigarea sigură pe internet. Disponibil la:
<https://www.tirnaveni.ro/sfaturi-pentru-navigarea-sigura-pe-internet/>
56. Siguranța online. Disponibil la:
https://sigurantaonline.ro/?fbclid=IwAR1UCwlo8DlaHfgzTDtyklb2AIWdtvNpVB2PYrvrFQj6zi8ieRUERSRmuz_o
57. Siguranța online, POVEȘTI, Disponibil la:
<https://sigurantaonline.ro/povesti/>
58. Tips for Family Link from Google. Disponibil la:
https://services.google.com/fh/files/misc/google_families_familylinktips.pdf
59. UNICEF, Cyberbullying: Ce este și cum îi punem capăt? 10 lucruri pe care adolescenții vor să le știe despre cyberbullying. Disponibil la:
<https://www.unicef.org/moldova/articole/cyberbullying-ce-este-%C8%99i-cum-%C3%AEi-punem-cap%C4%83t>
60. UNICEF, Policy guidance on AI for children, 2.0 | NOVEMBER 2021. Disponibil pentru download direct, la:
<https://www.unicef.org/globalinsight/media/2356/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf>
61. United Nations, Convention on the Rights of the Child, Dreptul la confidențialitate
62. United Nations, Convention on the Rights of the Child, Interesul superior al copilului
63. Update on the Twitter Archive at the Library of Congress, December 26, 2017. Disponibil la:
<https://blogs.loc.gov/loc/2017/12/update-on-the-twitter-archive-at-the-library-of-congress-2/>
64. viva.com, Cum să recunoașteți și să vă protejați de furtul de identitate. Disponibil la:
<https://www.viva.com/ro-ro/blog/how-to-recognise-and-protect-yourself-from-id-theft>
65. Voiculescu Simona, Redactor-șef, avocatnet.ro, Libertatea de exprimare a copiilor este doar unul dintre drepturile „uite” ale acestora. Disponibil la:
https://www.avocatnet.ro/articol_44911/Libertatea-de-exprimare-a-copiilor-este-doar-unul-dintre-drepturile-%E2%80%9Euite-ale-acestora.html
66. Wikipedia, Cookie. Disponibil la:
<https://ro.wikipedia.org/wiki/Cookie>
67. Wikipedia, Date personale. Disponibil la:
https://ro.wikipedia.org/wiki/Date_personale
68. Wikipedia, Ransomware. Disponibil la:
[https://ro.wikipedia.org/wiki/Ransomware#:~:text=Ransomware%20este%20un%20software%20r%C4%83u,%E2%80%9D%20\(%C3%AE%20englez%C4%83%20ransom\).](https://ro.wikipedia.org/wiki/Ransomware#:~:text=Ransomware%20este%20un%20software%20r%C4%83u,%E2%80%9D%20(%C3%AE%20englez%C4%83%20ransom).)
69. Wikipedia, Wi-Fi. Disponibil la:
<https://en.wikipedia.org/wiki/Wi-Fi>
70. Wind Discovery, Cum să-ți “tratezi” copilul de dependența de internet. Disponibil la:
<https://www.winddiscovery.ro/blog/tratare-dependenta-calculator/>
71. Zuky The Robot, Complex Passwords. Disponibil la:
https://www.youtube.com/watch?v=PeG_WRV9iQM&list=PLZ1IjQtA2fL11yY06-HnpsrJifRsYoeFg