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

TLP:CLEAR

Cuprins

I. INTRODUCERE 3
II. COPIII 8
II.1. Găsește un echilibru între distracție și siguranța ta online! 8
II.1.1. Ce sunt datele personale? 8
II.1.2. Ce este Cybersecurity (Securitatea Cibernetică)? 10
II.1.3. De ce este important să fii în siguranță în mediul online? 10
II.1.4. Ce este conștientizarea securității cibernetice? 10
II.1.5. La ce sunt folosite datele tale personale? 11
II.1.6. Gândește înainte de a da click! 11
II.1.7. Unde, cum și de către cine ar putea fi stocate (păstrate) datele tale? 12
II.1.8. Parolele 14
II.1.9. Ce știu dispozitivele tale despre tine? 14
II.1.10. Inteligența artificială în viața ta 16
II.1.11. Cum poți face navigarea pe internet sigură? 17
II.1.12. Cele mai comune și des întâlnite probleme cu care se confruntă copiii în mediul online 18
II.1.12.2. Furtul de identitate 21
II.1.12.3. Atacarea e-mail-urilor, a mesajelor sau a echipamentelor electronice (computer, laptop, tabletă, telefon mobil) 22
II.1.12.3.1. Phishing 23
II.1.12.3.2. USB Media 24
II.1.12.3.3. Social Engineering (inginerie socială) 25
II.1.12.3.4. Wi-Fi 26
II.2. Sfaturi utile pentru o navigare sigură pe internet 26
II.3. Drepturile tale - extras din “Drepturile copiilor” - Consiliul Europei 28
III. PĂRINȚII 31
III.1. Ce trebuie să știe părinții? 31
III.2. Cine ar trebui să le vorbească copiilor despre datele lor personale și securizarea acestora? 33
III.3. Ce trebuie să faceți când copiii accesează internetul? 34
III.4. Copiii și rețelele sociale 35
III.5. Care sunt principalele amenințări online? 38
III.6. Cum pot contribui la securitatea digitală a copilului meu? 39
III.7. Controlul parental – Gestionarea dispozitivelor (o problemă delicată) 42
III.8. Recomandări pentru părinți 43
IV. ȘCOALA ȘI PROFESORII 47
IV.1.Școala ca operator de date personale 47
IV.2. Ce înseamnă date personale ale elevilor? 48
IV.3. Aplicațiile și platformele educaționale 48
IV.4. Provocările Educației Online – cu ce ne putem confrunta? 50
IV.5. Cum să reacționăm la Cyberbullying? 51
IV.6. Școala și rețelele sociale 53
IV.7. Securizarea datelor cu caracter personal în cadrul educațional 53
V. CE FACEM ÎN CAZUL UNUI INCIDENT DE SECURITATE CIBERNETICĂ? RECOMANDĂRILE DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ (DNSC) 55
VI. BIBLIOGRAFIE 57

I. INTRODUCERE

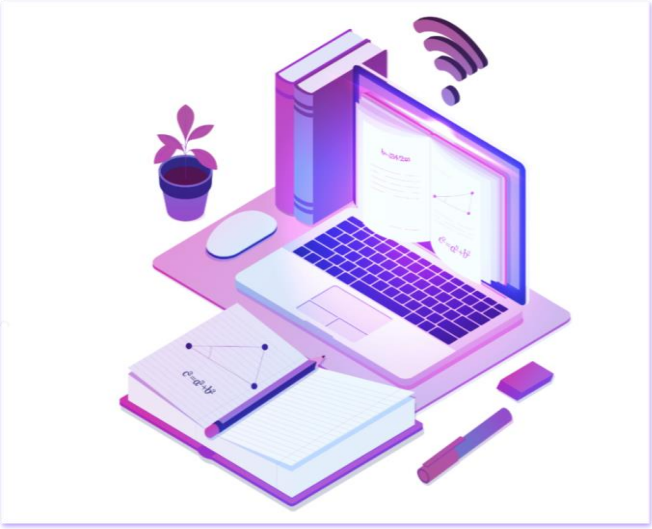
Prezentul ghid își propune să trateze subiectul confidențialității (privacy), a protecției datelor (data privacy) și a securității cibernetice (cybersecurity) a copiilor în mediul online.

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 prelucrează 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%83t

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/DetaliiDocument/156097

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

o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil."[4]

Confidențialitatea este vitală pentru libertatea, demnitatea și siguranța copiilor și pentru exercitarea drepturilor lor. Datele personale ale copiilor sunt prelucrate pentru a le oferi beneficii educaționale, de sănătate sau alte beneficii care pot contribui la dezvoltarea lor armonioasă. Amenințările la adresa confidențialității datelor copiilor pot apărea din colectarea și prelucrarea datelor personale de către instituțiile publice, companii și alte organizații, precum și din activități criminale, precum furtul de identitate.

Amenințările pot apărea din surse multiple, cel mai frecvent întâlnite fiind:

- activitățile proprii ale copiilor: navigare pe internet, jocuri online, socializare în mediul virtual, mai ales pe rețelele de socializare etc.;
- activitățile membrilor familiei: publicare/partajare de informații și material media (text, fotografii, clipuri, înregistrări audio-video etc.) cu și/sau despre un copil etc.;
- activitățile altora: colegi, profesori sau străini care împărtășesc informații și material media cu și/sau despre un copil, indiferent dacă informațiile au fost obținute din interacțiunea directă cu copilul sau provin din alte surse.[5]

Supravegherea digitală a copiilor și orice prelucrare automată asociată a datelor personale trebuie să respecte dreptul copilului la viață privată. Aceasta nu trebuie să fie efectuată în mod constant, discriminatoriu sau fără știrea copilului, iar în cazul copiilor foarte mici, fără știrea părinților sau a tutorilor acestora.
Supravegherea digitală a copiilor nu ar trebui să aibă loc fără a se respecta dreptul acestora de a se opune unei astfel de supravegheri în medii comerciale, în medii educaționale și de îngrijire și ar trebui să se ia întotdeauna în considerare mijloacele cele mai puțin intruzive disponibile pentru respectarea confidențialității lor.

Mediul digital ridică probleme deosebite părinților în ceea ce privește respectarea dreptului copiilor la viață privată. Tehnologiile care monitorizează activitățile online din motive de siguranță, cum ar fi dispozitivele și serviciile de urmărire, dacă nu sunt implementate cu atenție, pot împiedica un copil să acceseze o linie de asistență dedicată lor (**119 - "telefonul copilului"**, număr unic la nivel național) spre exemplu, ceea ce ar putea însemna, într-un anumit context, că sănătatea, integritatea fizică și psihică sau chiar viața unui copil ar putea fi puse în pericol.

Părinții și/sau cei care au copiii sub supraveghere ar trebui să fie sfătuiți cu privire la practicile prin care pot respecta și proteja intimitatea copiilor în raport cu mediul digital, păstrându-i în același timp în siguranță.

Monitorizarea, de către părinți, a activității digitale a unui copil ar trebui să fie proporțională și în conformitate cu vârsta și cu etapa de dezvoltare în care se află acesta (nu impunem același nivel de control parental unui adolescent în vârstă de 15 ani, așa cum am proceda cu un copil de 8-9 ani).

[4] Regulamentul 679/2016, art. 12, alin. 1. Disponibil la:
https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=RO

[5] United Nations, Convention on the Rights of the Child, pct. E, Dreptul la confidențialitate, 67

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 rezonabile[6], 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 servicii[7] 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:

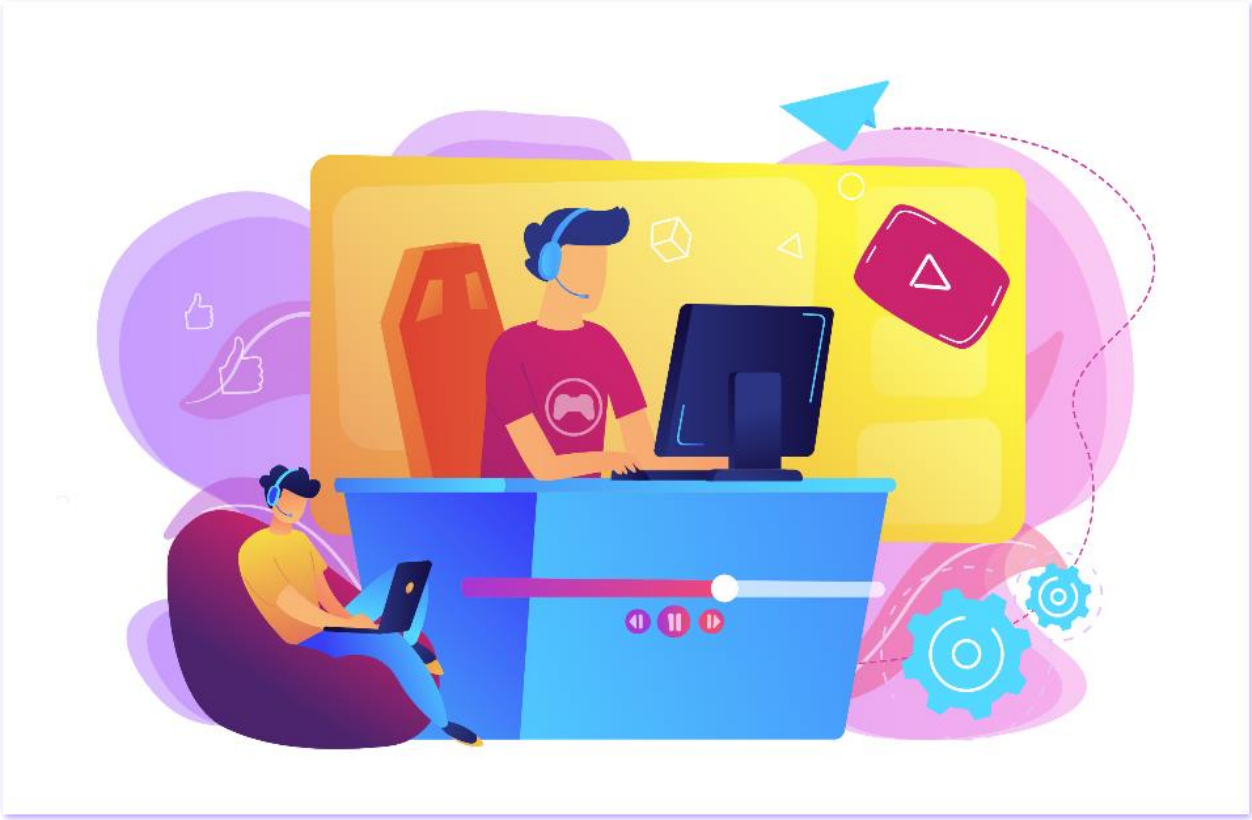
https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=02D734A02B6F26FB4E23F888E5A350C6?docid=183363&text=&doclang=RO&pageIndex=0&cid=1849533

[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

personalitate sau de utilizator și la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor.“[9]

Considerentul (58) arată că “*Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.*”[10]

Dat fiind faptul că există necesitatea de a avertiza atât copiii, cât și părinții, dar și școala, asupra pericolelor din mediul online, de a le face cunoscute drepturile de care se bucură copiii ca persoane vizate, dar și pentru a arăta cum pot fi aceștia protejați în lumea virtuală, s-a născut ideea acestui ghid care își propune să trateze subiectul protecției datelor personale, adresându-se copiilor, părinților, dar și profesorilor și școlii.



[9] *Ibidem*, considerentul (38)

[10] *Ibidem*, considerentul (58)

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

II. COPIII

II.1. Găsește un echilibru între distracție și siguranța ta online!

Când mergi pe bicicletă, porți o cască pentru a-ți proteja capul. Când înoți, porți ochelari de protecție pentru a-ți proteja ochii. Și atunci când folosești internetul ar trebui întotdeauna să-ți protejezi informațiile personale. Aceasta include să fii atent la ce și cui împărtășești, ce îți place sau nu, ce cumperi, cine sunt prietenii tăi, unde mergi la școală și multe alte informații.

De ce nu ar trebui să împărtășești aceste informații? Pentru că există persoane necunoscute și companii care le pot folosi pentru a câștiga bani sau, mai rău, pentru a-ți face rău ție sau familiei tale. Dar, uneori ești forțat să dezvălui online detalii precum numele tău complet și data nașterii. De unde știi dacă dai prea multe informații? Acest ghid este despre găsirea echilibrului între a te distra sau informa pe internet și a te proteja în același timp.

II.1.1. Ce sunt datele personale?

Datele cu caracter personal[11] reprezintă orice informație care se referă la o persoană vie identificată sau identificabilă (diferitele informații, colectate împreună, pot duce la identificarea unei anumite persoane). Cu alte cuvinte, datele cu caracter personal sunt informații despre tine sau despre alte persoane care pot fi folosite pentru a te/a le identifica.

De exemplu, numele tău, adresa unde locuiești, adresa ta de e-mail sau chiar locația ta de pe telefonul mobil sunt date cu caracter personal. În schimb, un număr de înregistrare al companiei sau o adresă de e-mail generală (de exemplu, info@companie.ro) nu sunt considerate date cu caracter personal.[12]

Dacă aceste informații sunt criptate sau amestecate într-un fel special, ele rămân tot date cu caracter personal și trebuie protejate. Totuși, dacă aceste informații sunt transformate într-un mod care face imposibilă identificarea cuiva, atunci ele nu mai sunt considerate date cu caracter personal.

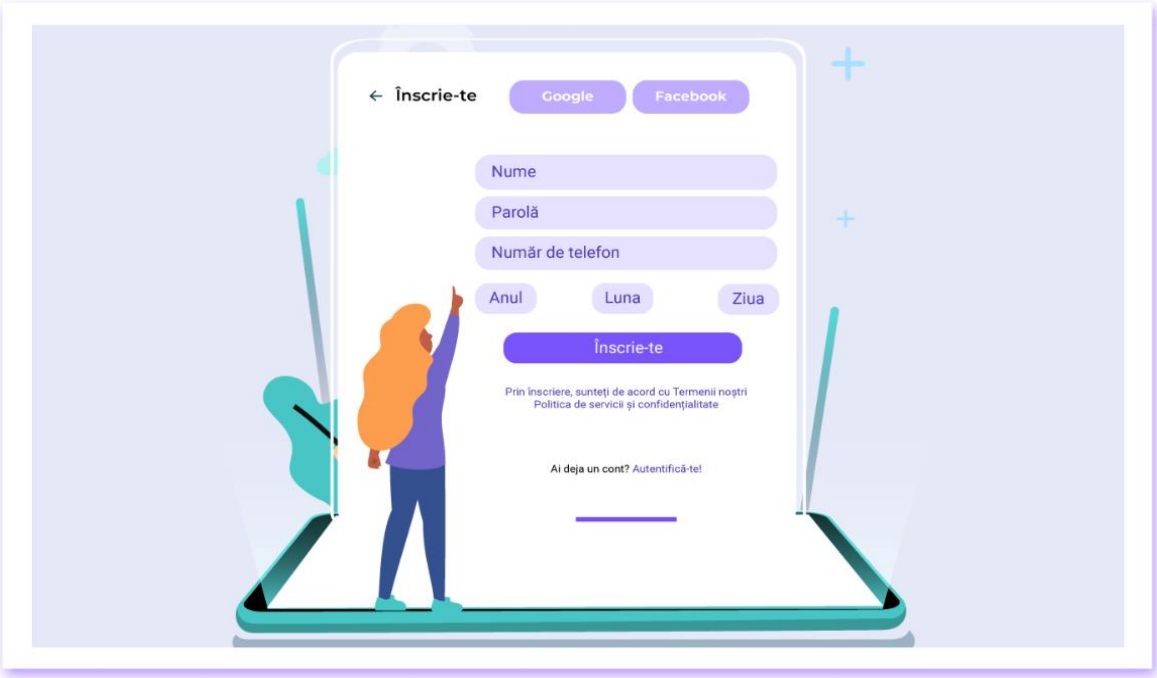


Figura 1 Solicitarea datelor personale cum ar fi numele, numărul de telefon și data nașterii.

[11] European Commission, *What is personal data?* Disponibil la: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

[12] *Ibidem*

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

Știai 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!

Știai 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.

II.1.2. Ce este Cybersecurity (Securitatea Cibernetică)?

Cybersecurity[13] sau securitatea cibernetică, este ca un gardian digital care păzește informațiile, rețelele și programele noastre împotriva hoților și răufăcătorilor online.

Imaginează-ți că internetul este ca un oraș minunat, plin de locuri distractive și lucruri interesante de descoperit. Dar, la fel ca în orice oraș, există și niște bandiți digitali care vor să fure sau să strice lucrurile bune ale orașului. Aici intervine securitatea cibernetică!

Acești eroi ai securității cibernetice pun la cale planuri inteligente și folosesc arme speciale digitale pentru a proteja casele noastre digitale (cum ar fi computerele, telefoanele sau tabletele noastre) și pentru a ne ajuta să navigăm în siguranță prin acest oraș virtual minunat. Ei se asigură că parolele noastre sunt puternice și că fișierele noastre sunt încuiate într-o cutie virtuală rezistentă, pentru a nu fi accesate fără permisiunea noastră.

În plus față de protejarea datelor și a jocurilor noastre online, securitatea cibernetică ne învață, de asemenea, cum să fim prudenți și să ne protejăm de pericolele de pe internet. De exemplu, ne învață să nu dăm click pe linkuri ciudate sau să nu descărcăm fișiere de la surse necunoscute, pentru că ar putea fi capcane puse de monștrii digitali.

În concluzie, securitatea cibernetică este ca un gardian digital, un prieten de nădejde care lucrează din greu pentru a ne păstra în siguranță în orașul minunat al internetului!

II.1.3. De ce este important să fii în siguranță în mediul online?

Siguranța în mediul online este importantă pentru că ne permite să rămânem protejați în activitățile pe care le desfășurăm pe internet și anume:

- Ne protejează informațiile personale: ne ajută să păstrăm secret numele nostru, vârsta sau alte lucruri despre noi, astfel încât orice persoană rău intenționată să nu poată să le folosească împotriva noastră.
- Suntem în siguranță când ne jucăm: ne asigură că jocurile și site-urile pe care le vizităm sunt potrivite pentru vârsta noastră și nu ne expun la lucruri neplăcute sau periculoase.
- Ne protejează împotriva persoanelor răuvoitoare: ne ajută să ne ferim de străinii care ar putea să ne contacteze sau să ne abordeze în mod nedorit, protejându-ne, în acest fel, de pericolele pe care le putem întâlni online.
- Previne bullying-ul online: ne învață cum să recunoaștem și să evităm situațiile în care cineva încearcă să ne rănească sau să ne jignească pe internet.
- Păstrează securitatea în timp ce ne jucăm: ne protejează de jocurile sau aplicațiile care ar putea să ne ceară informații personale sau să ne expună la riscuri.

II.1.4. Ce este conștientizarea securității cibernetice?

Conștientizarea securității cibernetice înseamnă să învățăm cum să fim în siguranță în mediul online. Este ca atunci când înveți să traversezi strada doar când lumina semaforului arată culoarea verde. Ne învață să fim atenți la lucrurile rele care se pot întâmpla online și cum să ne protejăm datele și jocurile pe care le iubim. Asta înseamnă să știm să folosim parole puternice, să nu dăm click pe linkuri suspecte sau să nu descărcăm fișiere primite de la persoane necunoscute, pentru că acestea ar putea să ne facă rău. Învățăm să recunoaștem când cineva încearcă să ne păcălească sau să ne jignească pe internet și cum să cerem ajutor, de la persoane de încredere, atunci când avem nevoie.

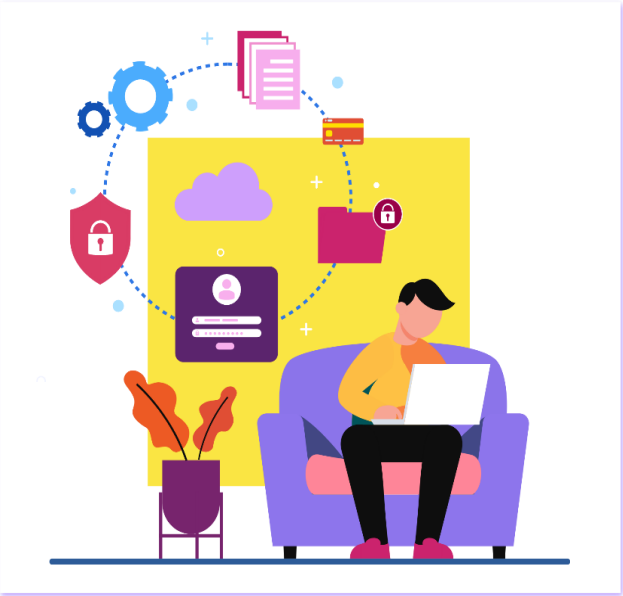
[13] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 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.RON&toc=OJ%3AL%3A2019%3A151%3ATOC

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:

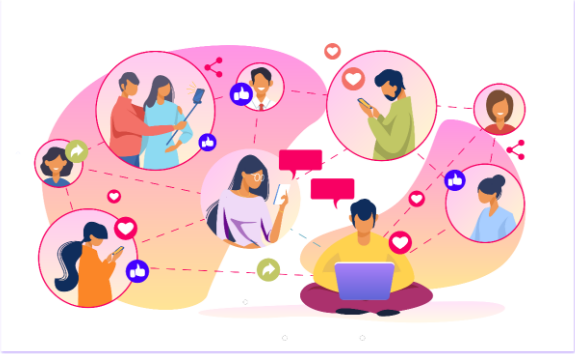
Securitatea cibernetică ne protejează datele și activitățile online de furt și alte amenințări. Este important să păstrăm informațiile personale în siguranță, pentru a evita jocurile și site-urile inadecvate și pentru a preveni contactul cu persoanele răuvoitoare. Conștientizarea securității cibernetice 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

NU uita!

- Nu posta nimic din ceea ce nu vrei ca un părinte, profesor sau cineva pe care îl admiri să vadă. Ești primul care îți poate proteja cel mai bine intimitatea și viața privată, fiind foarte atent și responsabil la ceea ce "arunci" despre tine în mediul online.
- Ai răbdare! Înainte de a posta ceva, orice, fie despre tine, fie despre alții, ia o pauză și gândește-te cât de sensibile sunt informațiile respective și dacă ți-ar putea dăuna ție sau altora!
- Când postezi ceva ce ți se pare amuzant, gândește-te dacă acea postare ar putea să-i jignească pe alții. Dacă tu crezi că există cel mai mic risc să faci rău altora, atunci NU posta! "Ce ție nu-ți place, altuia nu-i face!"

II.1.7. Unde, cum și de către cine ar putea fi stocate (păstrate) datele tale?

În momentul în care ai dat datele tale personale cuiva, indiferent cui și indiferent pentru ce motiv, dar, mai ales dacă le-ai "dat drumul" pe internet, poți să te aștepți ca datele tale să ajungă în locuri în care nici cu gândul nu gândești și să pierzi complet controlul asupra a ceea ce se întâmplă cu ele și cum ar putea fi folosite de alții.

Twitter și Biblioteca Congresului Statelor Unite

Doar cu titlul de exemplu și ca să-ți poți face tu o idee pe unde ar putea ajunge datele tale personale, îți vom spune povestea unui "cadou" pe care Twitter l-a făcut Bibliotecii Congresului Statelor Unite în anul 2010 și implicațiile acestuia. Twitter a fost o rețea de socializare, cu înscriere și acces gratuit, în care utilizatorii difuzau postări scurte cunoscute sub numele de tweet-uri. Aceste tweet-uri conțineau text, videoclipuri, fotografii sau link-uri.

În anul 2010, compania Twitter. Inc oferea "**cadou**" Bibliotecii Congresului Statelor Unite o colecție constând în toate tweet-urile/postările publice făcute pe respectiva rețea de socializare, de la crearea acesteia, până la data intrării în vigoare a acordului respectiv (iulie 2006 - aprilie 2010), dar și după data încheierii documentului menționat (Biblioteca a renunțat la "cadou" în data de 31.12.2017).[15]

Pentru mersul înainte al științei, pentru a documenta realizările omenirii la un moment dat, sau pentru o anumită perioadă, chiar dacă este vorba despre o rețea de socializare, nu este nimic în neregulă cu acest "cadou" primit de o bibliotecă. Ce este în neregulă, însă, este faptul că Twitter a acționat ca **proprietar** al informațiilor făcute cadou, deoarece se considera acoperit de "Termenii și condițiile" pe care utilizatorii sunt obligați să le accepte, dacă vor să folosească un anumit serviciu, inclusiv când vor să-și facă un cont pe o rețea de socializare.

Ce înseamnă asta? Înseamnă că utilizatorii, atunci când și-au creat contul pe Twitter, ori nu au citit deloc, ori nu au înțeles adevăratele consecințe ale acceptării termenilor și condițiilor, dar, "semnând de acceptare", au fost de acord că, implicit, tot ce postează ei pe Twitter, pe panoul public, devine proprietatea Twitter, iar compania poate face ce dorește cu acele informații (să le vândă, sau, ca în cazul de față, să le dăruiască). Atenție, au fost făcute cadou TOATE postările, indiferent de limba în care au fost făcute, sau indiferent cine le-a creat!

Cu alte cuvinte, când îți creezi un cont "gratuit" de e-mail, pe Yahoo, sau Gmail, sau pe rețelele de socializare ca Facebook, Instagram etc., tu, de fapt, "plătești" cu datele tale personale, care sunt un fel de plată "invizibilă". Nu prea ești conștient de existența ei, dar ea bagă o mulțime de bani reali în buzunarele acestor companii, care pot vinde datele tale oricui, ori de câte ori vor, deoarece devin proprietarii datelor pe care le "plimbi" prin aceste platforme (conținutul mesajelor, atașamente, fotografii, link-uri, înregistrări audio-video, comentarii, opinii etc.).

[15] 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/

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.

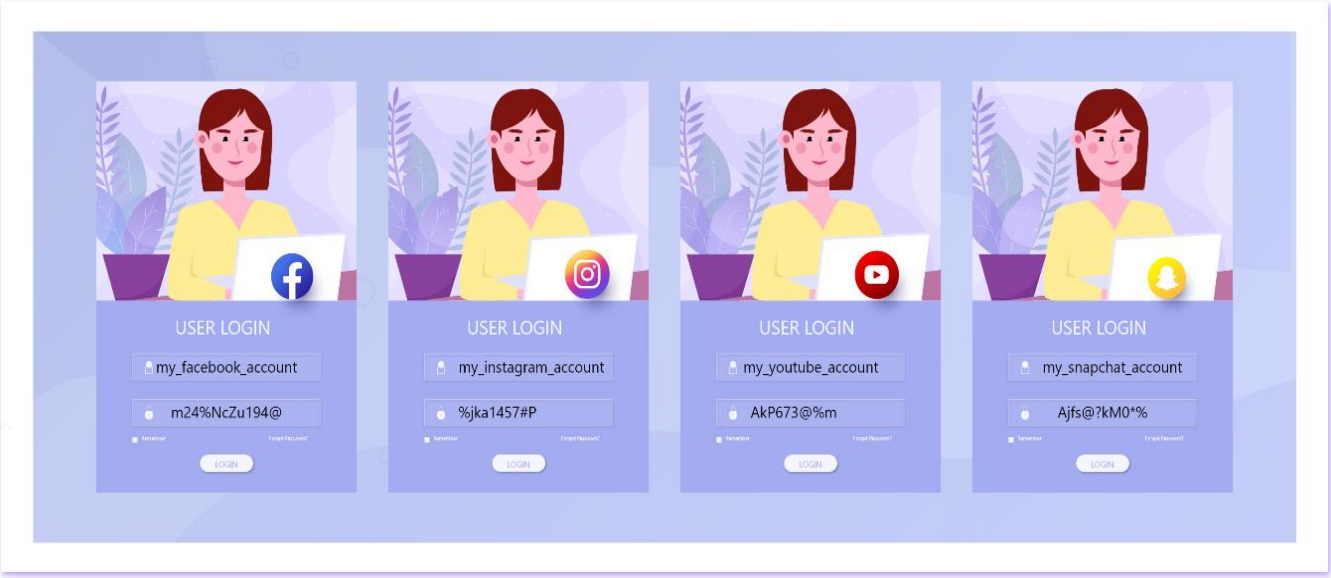
Rețelele de socializare

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 necazuri, 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 distorsionat, 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 gândi 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.

II.1.8. Parolele



Iată cum poți să-ți creezi o parolă puternică și să-ți protejezi conturile online:

- Alege o parolă complexă: Folosește o combinație de litere mari și mici, cifre și caractere speciale (% $ ^ # & etc.). Cu cât mai lungă și mai variată este parola, cu atât mai greu este pentru răuvoitori să o ghicească.
- Folosește parole separate pentru fiecare cont: Nu folosi aceeași parolă pentru toate conturile tale online. Dacă una dintre platforme este compromisă, parola ta va fi expusă pentru toate conturile. A ține evidența mai multor parole poate fi enervant, dar este important pentru securitatea ta.
- Activează Autentificarea în doi pași (2FA): Multe platforme oferă opțiunea de a activa 2FA. Acest lucru adaugă un nivel suplimentar de securitate, cerându-ți să introduci un cod unic trimis prin SMS sau generat de o aplicație de autentificare înainte de a putea accesa contul. Asigură-te că activezi 2FA oriunde este posibil pentru o securitate mai puternică.

Amintește-ți că este important să-ți protejezi datele personale și conturile online. Prin urmare, creează parole puternice și folosește alte măsuri de securitate disponibile pentru a-ți proteja identitatea online.

II.1.9. Ce știu dispozitivele tale despre tine?

Fie că vorbim despre computerul sau laptopul de pe biroul tău, fie că vorbim despre telefonul din buzunarul tău, echipamentele respective reține și prelucrează multe date personale. Toate aceste informații se pot dovedi vulnerabile în fața criminalității cibernetice. Datele personale au valoare monetară, adică sunt "vânate" pentru că se pot transforma în bani reali.

Dar despre ce fel de date personale este vorba?

Cele mai căutate date personale sunt:

- **Parolele** salvate în browser sau stocate în fișiere de sistem;
- Detaliile **cardurilor** de credit/debit cu care faci plăți online și pe care le salvezi în echipament sau în browser;
- Detalii despre **conturile** bancare;

- 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 ți 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 moment rescrierii fizice a echipamentului - momentul în care se formatează 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, MacIOS 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.certsign.ro/ro/10-trucuri-pentru-securizarea-telefonului-mobil/

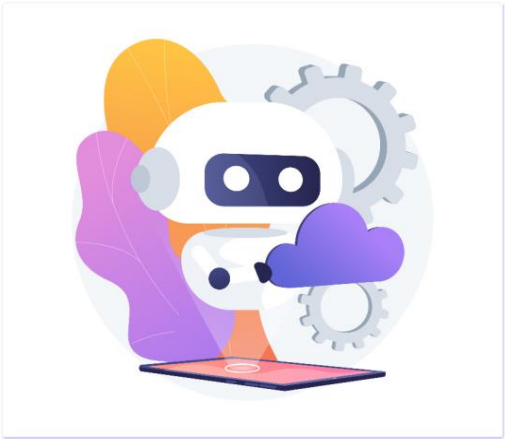
5. Verifică permisiunile aplicațiilor: Acordă atenție permisiunilor solicitate de aplicațiile pe care le descarci și asigură-te că sunt justificate pentru funcționalitatea aplicației.
6. Instalează actualizările de sistem: Actualizează periodic sistemul de operare al telefonului tău pentru a beneficia de cele mai recente patch-uri de securitate.
7. Fii atent la link-uri suspecte: Nu accesa linkuri sau atașamente din mesaje sau emailuri necunoscute sau suspecte.
8. Criptează datele de pe telefon: Activează criptarea pentru datele de pe telefonul tău pentru a le proteja împotriva accesului neautorizat.
9. Dezactivează conectarea automată la rețele Wi-Fi: Evită conectarea automată la rețele Wi-Fi publice și necriptate pentru a preveni accesul neautorizat la datele tale.
10. Dezactivează conectarea automată la Bluetooth: Evită conectarea automată la dispozitive Bluetooth necunoscute sau nesigure pentru a proteja datele și informațiile personale.

Respectând aceste recomandări, vei putea să-ți protejezi în mod eficient datele și intimitatea atunci când utilizezi telefonul mobil.

II.1.10. Inteligența artificială în viața ta

Tehnologia inteligenței artificiale (AI) face parte din viața de zi cu zi și oferă multe oportunități interesante dar, de asemenea, poate crea probleme sau le poate agrava, dacă nu este dezvoltată sau utilizată în mod responsabil. Tehnologia AI include computere și mașini programate să efectueze sarcini care imită modul în care oamenii gândesc și se comportă, executând activități complexe prin procese automate.

Tehnologia este utilizată pentru a prevedea evenimente specifice (de exemplu, traiectoria de răspândire a unui virus) sau pentru a sugera opțiuni (de exemplu, următoarele videoclipuri pe care să le urmărești online). Inteligența artificială operează în mai multe feluri: fie urmând un set de instrucțiuni definite într-un sistem (un algoritm), fie 'învățând' din analiza unei mase enorme de date (cum ar fi performanța ta academică, istoricul tău medical, istoricul căutărilor și așa mai departe) sau prin metoda 'trial and error' (nu întotdeauna inteligența artificială produce răspunsul exact sau cea mai bună soluție, și, prin urmare, procesând date adiționale, se 'perfecționează' și reduce probabilitatea de a repeta aceleași erori).



Datele pe care sistemele AI le folosesc ar putea proveni din tot felul de surse, cum ar fi înregistrări de voce, din text, din imagini sau din videoclipuri etc., adică de oriunde i se permite accesul. Sistemele AI caută relații (conexiuni logice) între aceste date și stabilesc modele (tipare), adică pun cap la cap informații aparent fără nicio legătură între ele, dar care capătă sens doar când sunt aduse împreună. Când tehnologiile AI descoperă un tipar, ele interacționează cu noi oferind un răspuns, recomandându-ne să luăm anumite decizii.

Tehnologia poate fi folositoare sau dăunătoare, depinde de cine o creează și cum este utilizată.

Spre exemplu, aplicațiile AI te pot ajuta să-ți dezvolți noi abilități, să îți îmbunătățești vocabularul și să-ți dezvolți cunoștințele generale, sau pe cele specifice unei discipline școlare. Cu toate acestea, sistemele AI au nevoie de un volum extrem de mare de date pentru a învăța și,

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 recomandări[21]:

- 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, respecți 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/

le imediat! În acest fel îți protejezi viața personală și nici nu riști să-ți fie folosite conturile pentru a face rău altora;

- NU folosi numele tău întreg, data nașterii, elemente din adresa ta sau orice alte informații sau bucăți de informație personală care ar putea fi cunoscute/recunoscute/asociate cu persoana ta, atunci când îți creezi adresa de e-mail, ci folosește un pseudonim sau o prescurtare;
- NU stabili parole simple, doar pentru că le reții mai ușor! Parola ar trebui să conțină cel puțin 12 caractere, combinând litere, cifre și semne speciale. În niciun caz nu folosi data ta de naștere, sau a prietenei/prietenului tău, numele animalului tău de companie, porecle pe care ți le cunosc și alții etc.;
- NU deschide atașamente primite pe e-mail fără să le scanezi (antivirus) mai întâi;
- NU descărca și nu instala programe fără licență/programe piratate. Nu faci economie la bani și mai riști și să-ți virusezi sau chiar să-ți strici calculatorul;
- NU salva parolele în browser și nu permite acestuia să rețină date de identificare sau să accepte transmiterea de date dacă sunt solicitate ca fiind "în interes statistic" etc.;
- NU continua navigarea pe internet sau o discuție pe chat, dacă s-a întâmplat ceva ce nu ți-a plăcut sau te-a speriat. Blochează pagina respectivă sau părăsește acel grup de chat;
- NU deschide și șterge imediat orice e-mail-uri, fișiere, fotografii sau programe de instalare primite de la cineva pe care nu-l cunoști sau care ți se par suspecte. Cere ajutorul unei persoane specializate când observi că nu mai funcționează normal calculatorul;
- NU comunica decât cu persoane de încredere atunci când ai camera web pornită. Cel puțin, folosește un fundal care să nu permită să se vadă ce se întâmplă în casă la tine. Răufăcătorii pot vedea dacă ai lucruri de valoare, pot afla dacă și când este cineva acasă, te-ar putea păcăli să faci lucruri ca să te poată șantaja sau să-i lași să intre în casă la tine;
- NU accepta și nu te duce la întâlniri față în față cu cineva cunoscut pe Internet. Anunță un adult de încredere imediat ce ți s-a făcut o asemenea propunere.

II.1.12. Cele mai comune și des întâlnite probleme cu care se confruntă copiii în mediul online

În data de 09.02.2021, Institutul de Cercetare și Prevenire a Criminalității, aflat în subordinea Inspectoratului General al Poliției Române, a publicat Raportul de cercetare "*Riscuri și vulnerabilități ale elevilor în mediul online*", întocmit în urma unui studiu derulat pe parcursul anului 2020 și care și-a propus "identificarea principalelor riscuri și vulnerabilități cu care se confruntă elevii cu vârste cuprinse între 10 și 18 ani din România în mediul online (în principal pornografie infantilă și atacuri cibernetice), tipologii ale victimelor și infracționale, moduri de operare etc."[22]

Printre obiectivele cercetării s-au aflat studierea evoluției fenomenului criminalității informatice, cu accent pe atacurile cibernetice cu victime minori și pornografia infantilă (dimensiunea problemei), obținerea unei descrieri a obiceiurilor de utilizare a internetului de către copii și a comportamentului acestora pe internet, dar și evaluarea gradului de cunoaștere și de utilizare a măsurilor de siguranță de către minori în utilizarea internetului.

Studiul este foarte amplu și recomandăm parcurgerea lui în întregime și, dacă nu înțelegi ceva din ce scrie acolo, îți recomandăm să soliciți ajutorul unui adult, deoarece informațiile prezentate

[22] 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

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 "știu 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/recâștigării 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

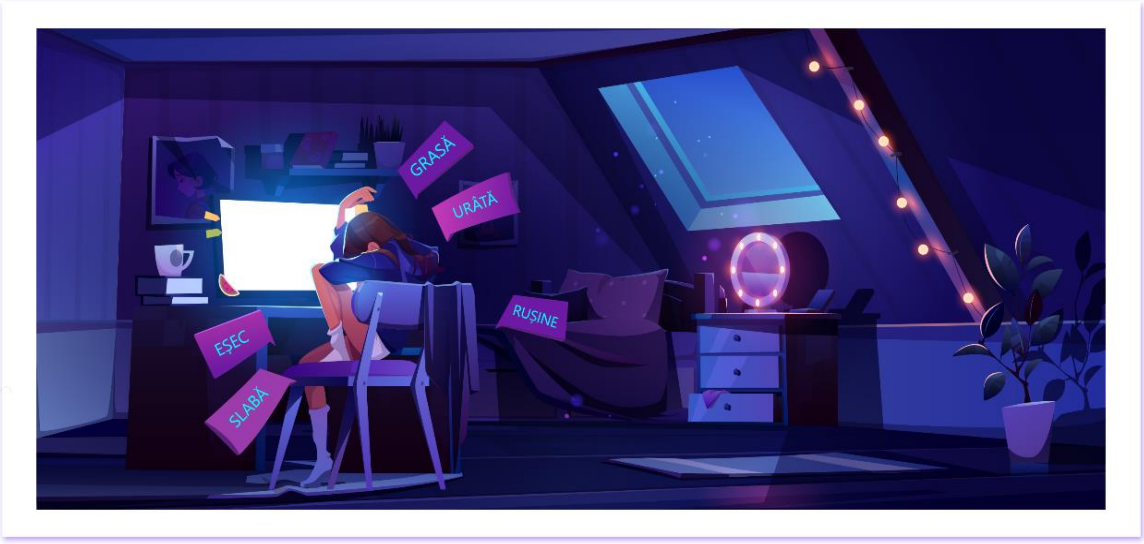
26 Ibidem.

27 Ibidem.

Dorim să-ți atragem atenția că niciuna din situațiile prezentate mai sus nu este în regulă și îți recomandăm foarte serios să eviți pe cât posibil să fii atras în asemenea întâmplări, dar, și dacă se întâmplă să greșești, să nu-ți fie teamă și să contactezi cât mai repede un adult în care ai încredere și să-i ceri ajutorul.

II.1.12.1. Prădătorii cibernetici și hărțuirea în mediul online (cyberbullying)

Cyberbullyingul[28] se manifestă atunci când cineva folosește tehnologiile digitale, cum ar fi telefoanele mobile sau rețelele de socializare, pentru a face rău sau a intimida pe altcineva în mod repetat.



De exemplu, poate fi trimis un mesaj răutăcios pe internet sau poate fi distribuită o fotografie jenantă a unei persoane fără permisiunea acesteia. Este important să vorbești cu un adult în care ai încredere dacă te simți intimidat sau dacă întâlnești astfel de situații pe internet. Acest lucru te poate ajuta să obții ajutor și să pui capăt comportamentului de cyberbullying.

Dacă te temi pentru siguranța ta sau pentru ceva ce ți s-a întâmplat în mediul online, vorbește imediat cu un adult în care ai încredere. Sau accesează Child Helpline International pentru a identifica mijloace de ajutor pe care le ai la dispoziție în țara ta.

Accesând pagina web de la UNICEF[29], găsim cele mai importante 10 întrebări despre cyberbullying. Aceste întrebări își propun să ofere o mai bună înțelegere a fenomenului și să ofere soluții pentru prevenirea și gestionarea acestuia:

1. *Sunt hărțuit(ă) în mediul online? Cum faci diferența dintre o glumă și bullying?*
2. *Care sunt efectele agresiunii de tip cyberbullying?*
3. *Cu cine ar trebui să vorbesc dacă cineva mă agresează în mediul online? De ce este important să raportezi?*
4. *Mă confrunt cu cyberbullying, dar îmi este teamă să le vorbesc părinților mei despre asta. Cum să îi abordez?*
5. *Cum îmi pot ajuta prietenii să raporteze un caz de cyberbullying, mai ales atunci când ei nu vor să o facă?*
6. *Cum putem pune capăt cyberbullyingului, fără a renunța la accesul la internet?*
7. *Cum pot preveni folosirea informațiilor mele personale în scopul manipulării sau umilirii mele pe rețelele de socializare?*

[28] 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/romania/ro/pove%C8%99ti/cyberbullying-ce-este-%C8%99i-cum-%C3%AEi-punem-cap%C4%83t

[29] 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/romania/ro/pove%C8%99ti/cyberbullying-ce-este-%C8%99i-cum-%C3%AEi-punem-cap%C4%83t

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 dubiu[30]:

- 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 (Ionel 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

Această situație se încadrează la furtul de identitate, deoarece persoana care a furat datele cardului lui Alex se dă drept acesta pentru a cumpăra lucruri, online. Este important să păstrăm informațiile personale în siguranță și să nu le împărtășim cu persoane necunoscute, fie online sau offline.

Dacă cineva îți cere informații personale sau dacă observi că banii tăi dispar din cont fără să știi de ce, spune asta, imediat, unui adult de încredere. Furtul de identitate este o infracțiune, este ilegal și este pedepsit în orice țară, inclusiv în România.

Moduri în care ți se poate fura identitatea[31]

Din păcate, furtul de identitate nu este chiar așa de greu de realizat, dacă nu ești atent. Niciun hoț nu-ti poate fura datele dacă nu-l ajuți si tu, prin neatenție și/sau din neglijență.

Unele dintre cele mai comune metode de furt utilizare de către atacatori sunt frauda prin e-mail (Phishing), apel telefonic (Vishing) și SMS (Smishing). Cu toate acestea, se poate fura identitatea utilizând doar informațiile disponibile public pe internet sau pe rețelele de Wi-Fi nesigure[32].

O metodă ușoară de a ți se fura identitatea? O persoană răuvoitoare postează o reclamă la o excursie gratuită, sau la un mega/mare/nemaipomenit/nemaivăzut premiu și ți se cere să furnizezi un document de identitate ca să-ți rezervi locul și să-ți revendici premiul. Citești acest text și îți spui: „Mie nu mi se poate întâmpla, eu sunt precaut!” Chiar n-ai fost tentat niciodată? Chiar crezi că toți sunt ca tine? Dacă n-ar fi și naivi, nu am mai discuta acum despre furtul de identitate.

Să mergem mai departe și să-ți povestim cum mai pot fi folosite actele tale de identitate: se creează o adresă de e-mail care să conțină numele tău, se pune poza altcuiva peste actul tău de identitate și se folosește pentru tot felul de ilegalități, mai ales că, în zilele noastre, poți să deschizi și un cont bancar, sau să obții un credit, fără să te mai deplasezi la bancă. Este suficient să se trimită o copie a actului de identitate și, eventual, să se furnizeze o adresă de e-mail pentru corespondență, validarea contului etc.

II.1.12.3. Atacarea e-mail-urilor, a mesajelor sau a echipamentelor electronice (computer, laptop, tabletă, telefon mobil)

Obținerea frauduloasă (ilegală) a accesului la dispozitivele sau conturile tale de e-mail sau de pe rețelele de socializare nu este chiar atât de dificilă pe cât pare. Când auzim de hackeri, ne imaginăm că ne atacă niște genii, cu niște tehnici și instrumente demne de filmele SF. Îți vom arăta, în continuare, că lucrurile nu stau deloc așa și că, în unele situații, este chiar foarte ușor să se întâmple aceste lucruri, pentru că, așa cum am spus și mai sus, îi ajutăm și noi, din plin, fiind neglijenți sau chiar neacordând atenție unor norme simple de securitate pe care le putem aplica și noi foarte ușor, dar nu o facem, pentru că ne gândim că “N-are nimeni ce să-mi fure/nu are ce să facă cu ceea ce am eu în cont” etc.

FALS! Absolut orice poate fi furat de la tine, în materie de informații și date personale, poate fi vândut și refolosit într-o mulțime de moduri periculoase despre care tu nici nu ai habar. Prin urmare, te rugăm să citești cu mare atenție cele ce urmează.

[31] MelsMine, *Ce este furtul de identitate*? Disponibil la: https://www.furtdeidentitate.ro/furtul-de-identitate/ce-este-furtul-de-identitate/

[32] 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

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 (viruși) 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 drăgălașă 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”.

Cum te poți proteja?

- Nu deschide email-uri nesolicitate, care provin de la persoane necunoscute. Nu le deschide nici dacă-ți vin de la prieteni, dar sunt reclame cu oferte prea frumoase să fie adevărate. E-mail-ul prietenului ar putea fi infectat și el să nu aibă habar că ai primit un asemenea mesaj de la el/ea. Te costă mai puțin să-l suni și să-l întrebi dacă mesajul primit este real și este ok. Nu-ți răspunde prietenul imediat? Nu intra în panică și nu te grăbi, crezând că pierzi măreața ofertă sau marele cadou, dacă nu dai click pe linkul respectiv în următoarele 5 minute sau în următoarea oră. Nu uita că acestea intră în categoria „E prea frumos să fie adevărat!" și „Nicio superofertă nu ține doar câteva minute/ore!".
- Nu deschide fișiere atașate și nu accesa linkurile din mesaje nesolicitate. Poți trăi și fără să vezi pozele sau filmulețele din atașamentul e-mailului sau fără să citești nemaipomenita poveste din documentul atașat sau de pe pagina unde te va duce linkul din corpul mesajului. Curiozitatea te poate costa foarte scump.
- Raportează și șterge email-urile nesolicitate.
- Folosește o soluție de securitate[33]

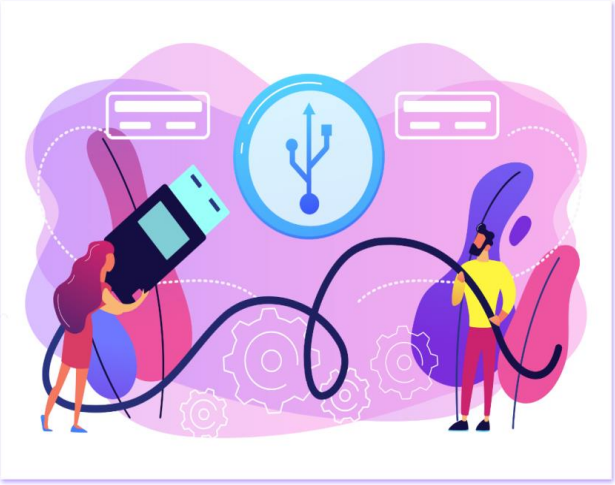
Ai grijă ...

- ce distribui pe internet despre tine;
- ce distribui pe internet despre alții;
- nu-ți expune preferințele și hobby-urile pe internet, fără discernământ;
- cine-ți este adevărat prieten îți cunoaște data nașterii și te felicită la telefon, nu pe Facebook, deci, ca să nu folosească cineva data ta de naștere ca să-ți facă rău, ai putea s-o ascunzi, să nu fie publică.

NU FACE CE ȚI SE CERE ÎN ACESTE MESAJE! ANUNȚĂ-ȚI PĂRINȚII, PROFESORII SAU UN ADULT DE ÎNCREDERE!

II.1.12.3.2. USB Media

Dintre toate gadget-urile care ne facilitează interacțiunile și comunicarea, probabil că Stick-ul USB Media pare cel mai inofensiv. De câte ori nu ni s-a întâmplat să copiem muzică sau filme pe un Stick de memorie pe care mai apoi să le împărtășim bucuroși cu prietenii, să le ascultăm în mașină sau acolo unde nu avem internet dar avem laptop sau computer sau chiar un televizor smart, astfel încât să ne putem relaxa ascultând sau vizionând fișierele stocate astfel. Iar când nu ne mai plac le putem șterge și înlocui foarte ușor cu altele. Singura problemă pe care o putem întâmpina ar fi ca, în memoria disponibilă pe Stick-ul USB media, să nu încapă tot ce am vrea noi să adăugăm.



Vreau să-ți aduc în atenție un exemplu din istorie pe care vreau să-l folosesc ca analogie, ca tu să poți înțelege pericolele pe care le pot prezenta cele mai neașteptate obiecte.

Imaginează-ți un vapor sau o corabie, care au fost și sunt mijloace de transport pe apă, pentru persoane și pentru mărfuri. Acestea sunt folosite de oameni pentru schimburi comerciale, asigurând printre altele, hrana populației și materiile prime pentru industrie.

[33] 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

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 contaminate[34].

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 transmițător 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.

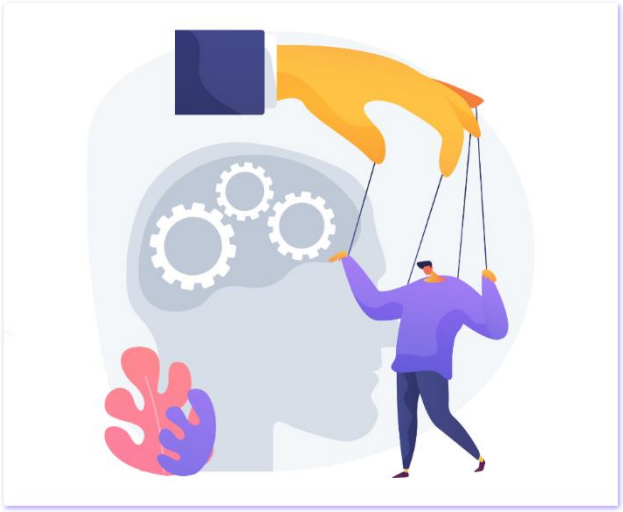
Apare, însă, firesc, întrebarea: Cum ne protejăm de virușii informatici în acest caz?

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 iezii 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] Medicover, Ciuma – o boala infecțioasă care încă nu a fost eradicată. Disponibil la: https://www.medicover.ro/despre-sanatate/ciuma-o-boala-infectioasa-care-inca-nu-a-fost-eradicata,1033,n,295

care le compromit securitatea dispozitivelor și aplicațiilor pe care le folosesc. Ingineria socială se bazează mai degrabă pe psihologie și pe comportamentul uman, decât pe know-how-ul tehnic[35].

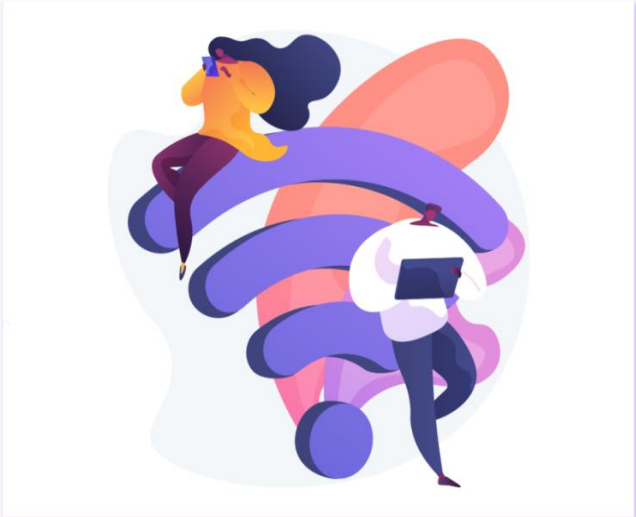
II.1.12.3.4. Wi-Fi

Prin acest ghid încercăm să te sfătuim cum să eviți neplăcerile create de folosirea noilor tehnologii, care riscă să-ți provoace daune materiale sau, poate chiar mai rău, prejudicii de imagine. Nu ești singurul care se întreabă cum este posibil ca ceva ce ne este atât de folositor, cum este Wi-Fi-ul, să ne poată produce și atâtea necazuri?

Ce este Wi-Fi și de câte tipuri este?

Tehnic vorbind, Wi-Fi este o familie de protocoale de rețea fără fir bazate pe familia de standarde IEEE 802.11, care sunt utilizate în mod obișnuit pentru rețelele locale ale dispozitivelor și accesul la Internet, permițând dispozitivelor digitale din apropiere să facă schimb de date prin unde radio[36]. Wi-Fi este, în esență, un radio digital foarte avansat, care utilizează frecvențe între 2 gigaherți și 5 gigaherți în spectrul electromagnetic[37].

Principala problemă cu securitatea rețelei wireless este accesul simplificat la rețea, în comparație cu rețelele tradiționale cu fir, cum ar fi Ethernet. Cu o rețea prin cablu, trebuie fie să obții acces la o clădire (conectându-te fizic la rețeaua internă), fie să obții acces printr-un firewall extern. Pentru a accesa Wi-Fi, trebuie doar să te afli în raza de acțiune a rețelei Wi-Fi. Majoritatea rețelelor de afaceri protejează datele și sistemele sensibile încercând să interzică accesul extern. Activarea conectivității wireless reduce securitatea, dacă rețeaua folosește o criptare inadecvată sau nu o folosește deloc.



Nu-ți vom da detalii despre securizarea rețelelor Wi-Fi deoarece este mult prea complicat pentru vârsta ta, dar îți spunem că cel mai bun mijloc prin care îți poți proteja și singur dispozitivele tale este să nu te conectezi la rețele cu acces liber, în gări, aeroporturi, restaurante, baruri etc.

II.2. Sfaturi utile pentru o navigare sigură pe internet

- *Fă-ți părinții "prieteni" pe internet!* Spune-le ce site-uri vizitezi, oamenii cu care schimbi mesaje sau e-mail-uri sau pe ce rețele sociale ai cont! Dacă primești un mesaj suspicios, ca cele din exemplele de mai sus, spune-le imediat!
- *Nu da niciodată date personale!* Dacă cineva te întreabă care este numele tău întreg, unde locuiești, la ce școală mergi, care este ziua ta de naștere sau îți cere informații despre persoanele apropiate, nu răspunde și anunță-ți imediat părinții!
- *NU alege un username care include informații personale!* Spre exemplu, dacă numele tău este Elena Rizea, ești născută pe 20 mai 2007 și locuiești în Brașov, nu face *ElenaRizea052007BV* username-ul tău! Poți fi campion la jocuri și fără să îți arăți identitatea!
- *Distribuie poze cu grijă!* Nu trimite străinilor, în mediul online, poze sau videoclipuri cu tine, familia sau prietenii tăi, casa sau școala ta!
- *Utilizează și verifică setările de confidențialitate* pe conturile de rețele sociale precum Facebook, Instagram, TikTok și Twitter!

---

[35] Consiliul European, Consiliul Uniunii Europene, Securitatea cibernetică: ingineria socială. Disponibil la: https://www.consilium.europa.eu/ro/policies/cybersecurity/cybersecurity-social-engineering/

[36] Wikipedia, Wi-Fi. Disponibil la: https://en.wikipedia.org/wiki/Wi-Fi

[37] Matthew Sparkes, *What does Wi-Fi stand for?* Disponibil la: https://www.newscientist.com/question/what-does-wi-fi-stand-for/

- *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 cățelului 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 descui. 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]

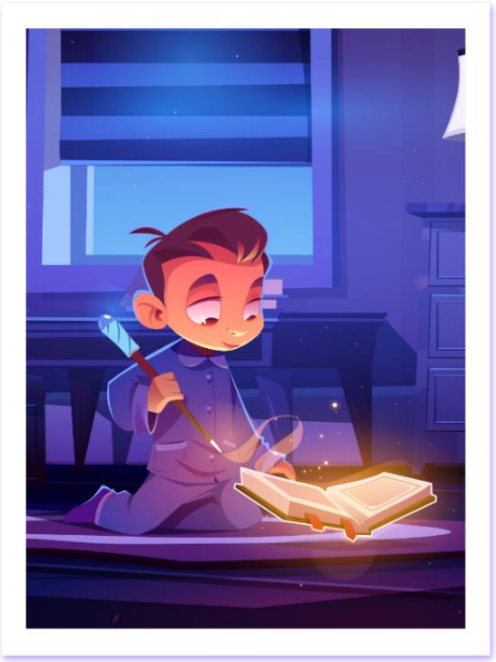
38 Zuky The Robot, *Complex Passwords*. Disponibil la:
https://www.youtube.com/watch?v=PeG_WRV9iQM&list=PLZ1IjQtA2fL11yY06-HnpsrJifRsYoeFq

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/

Exemple de video: https://saferkidsonline.eset.com/en-us/kids-zone

II.3. Drepturile tale - extras din "Drepturile copiilor" - Consiliul Europei

Supraviețuirea, protecția și dezvoltarea ta



- Ai dreptul ca interesele să-ți fie protejate în toate deciziile care te privesc și **pentru a nu fi supus(ă) discriminării**, spre exemplu, din cauza originii, opiniilor, convingerilor sau sexului tău.
- Ai dreptul la viață și la o dezvoltare fizică, mentală, spirituală, morală și socială echilibrată și sănătoasă.
- Ai dreptul la **protecție împotriva tuturor formelor de exploatare, abuz și violență fizică și psihologică**, inclusiv atunci când acestea sunt comise în interiorul familiei tale sau într-un mediu în care copiii sunt îngrijiți (școală, grădiniță, tabere, excursii etc.).
- Ai dreptul să ți se ofere o gamă largă de **informații obiective** despre orice te-ar putea interesa sau despre orice te-ar putea privi pe tine, într-un limbaj pe care tu să-l poți înțelege.
- Ai dreptul la odihnă, la timp liber, la joacă și activități recreative, artistice și culturale, **într-un mediu care să fie potrivit vârstei tale și să îți respecte drepturile**.

Identitatea, viața privată și familia ta

- Ai dreptul la un nume, o cetățenie și la **protejarea identității tale**. Dacă aparții unei minorități etnice, religioase sau lingvistice, nu poți fi privat(ă) de dreptul tău de a-ți trăi propria viață culturală, de a-ți practica religia sau de a utiliza limba grupului aparținător.
- Ai dreptul să-ți fie protejată intimitatea. Casa, corespondența, onoarea și reputația ta sunt protejate prin lege.
- Părinții tăi au o responsabilitate comună cu privire la creșterea și dezvoltarea ta. Aceștia au dreptul și sarcina de a-ți oferi îndrumare cu privire la modul în care trebuie să îți exerciți drepturile și să îți respecți obligațiile.
- În eventualitatea separării părinților tăi, ai dreptul să fii consultat(ă) cu privire la toate deciziile ce se referă la relația ta viitoare cu părinții (împreună sau cu fiecare dintre ei, în parte). Dacă ești separat(ă) de ambii părinți sau doar de unul dintre ei, ai dreptul să îi vezi periodic, exceptând situația în care acest lucru nu este în interesul tău (poți refuza să-i vezi, pe oricare dintre ei, mai ales dacă ai motive întemeiate pentru acest refuz; dacă unul sau oricare dintre părinți îți interzice să te întâlnești cu un necunoscut întâlnit în mediul online, iar tu nu ești de acord cu acest lucru, ba chiar te superi și te consideri nedreptățit și îngrădit, acesta nu este un motiv întemeiat să refuzi vizitele la părinții tăi; dar, dacă în timpul acestor vizite, ești abuzat, jignit sau exploatat în orice mod, atunci nu doar că ai un motiv întemeiat să nu vrei să-ți vizitezi părinții, ci, mai mult, poți povesti aceste lucruri celor care au grijă de tine și să soliciți ajutorul lor).
- Adopția poate fi autorizată doar dacă este în interesul tău.

Tu și statul

- Statul trebuie să facă tot ceea ce este necesar pentru a-ți permite să îți exerciți drepturile și libertățile stabilite prin lege.
- Statul trebuie să te protejeze și să îți asigure bunăstarea. Statul trebuie să-ți ajute părinții sau persoanele care te îngrijesc, înființând instituții și creând servicii care să servească intereselor și bunăstării tale.

- 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 nețărmurită 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]}

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

https://www.avocatnet.ro/articol_44911/Libertatea-de-exprimare-a-copiilor-este-doar-unul-dintre-drepturile-%E2%80%9Euitate-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.htp_act_text?idt=28213

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

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 rătăcească 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 anonimat, 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.

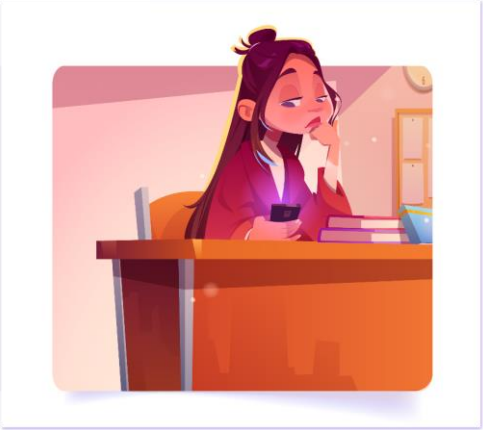
În general, răufăcătorii cibernetici încearcă să vă inducă în eroare copilul și să primească acces la datele sale personale, sau chiar și ale dvs. și/sau ale altor membri ai familiei, în special pentru câștig material, adică pur și simplu fac rost de marfă de vânzare pentru cumpărătorul potrivit (spre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

Totuși, există anumite tipuri de infractori extrem de periculoși care nu sunt interesați doar de beneficiile materiale ce ar putea proveni din reclamele direcționate către copiii dumneavoastră. Aceștia, de fapt, îi vizează direct pe copii pentru scopuri nelegale și grave, cum ar fi exploatarea minorilor, abuzul sexual sau traficul de persoane și organe.

Mulți copii se bucură de atenția pe care o primesc în mediul online și se lasă păcăliți, fie să dea și mai multe date personale, fie chiar să "iasă" din mediul online și să se întâlnească cu acești prădători în viața reală, fără ca dvs. să fiți conștienți de ce se întâmplă.

Din experiența noastră de specialiști în protecția datelor, dar și în calitate de părinți, am remarcat că părinții manifestă un interes din ce în ce mai crescut față de tematica protecției copiilor și a confidențialității datelor lor în online, în sensul în care părinții vor să cunoască modul cum se creează și care sunt consecințele amprentei digitale pe care copiii lor o lasă în mediul online.

În calitate de părinți, noi, autorii, am constatat că ne ajută să începem cu elementele fundamentale. Activitatea online de orice fel – jocuri, socializare pe diverse rețele dedicate acestui scop, navigare pe internet și așa mai departe – are potențialul de a lăsa o amprentă digitală. Având în vedere acest lucru, este util să împărțiți propria abordare a confidențialității datelor în două faze.



Faza 1: Evaluați toate serviciile online, site-urile, aplicațiile și dispozitivele care implică conectarea la internet și pe care copiii le folosesc și le accesează. Ce permisiuni dau, implicit, aplicațiile pentru smartphone-uri, adică, spre exemplu, este permis, implicit, ca datele personale să se transmită, automat, și către alți operatori, sau sunt folosite doar de proprietarii aplicațiilor respective? Care sunt setările de confidențialitate pentru conturile de pe rețelele sociale ale copiilor? Găsirea acestor informații poate fi o provocare.

Site-ul *internetmatters.org*[43] este o resursă excelentă pentru informații specifice despre următoarele (și multe altele):

- Cum să găsiți și să selectați setările de confidențialitate pe smartphone-uri și alte dispozitive, cum ar fi motoare de căutare, console de jocuri, rețele și aplicații etc.
- Unde să găsiți și să citiți politicile de confidențialitate și cerințele de vârstă pentru înregistrarea/crearea de conturi personale de utilizator pe o serie de platforme sociale, inclusiv TikTok, Facebook, Monkey, Instagram și multe altele.
- Unde și cum să raportați problemele sau preocupările dvs. legate de confidențialitate pe platformele de socializare.
- Studierea acestor resurse, împreună cu copiii dvs., este un punct de plecare excelent pentru următorul pas.

Faza 2: Evaluarea măsurilor de protecție a datelor copiilor în mediul online, prin discutarea cu aceștia a celor mai bune practici, precum și stabilirea unor limite:

- Ce fel de informații sau fotografii ale copiilor/despre aceștia sunt potrivite pentru partajare?
- Ce ar trebui să facă copiii dacă văd conținut care este supărător, le provoacă chiar și cel mai mic disconfort, fie că sunt, fie că nu sunt subiectul acestor conținuturi?
- Cum ar trebui să gestioneze solicitările străinilor de a se conecta pe rețelele sociale?
- Cum să facă distincția între adevăr și ficțiune în lumea digitală?

În acest moment, dvs., ca părinți, s-ar putea să vă dați seama că nu puteți verifica absolut toate interacțiunile copilului cu mediul online. Acesta este momentul în care vă puteți baza pe ajutorul legislației privind confidențialitatea datelor personale. Există soluții tehnice de accesare

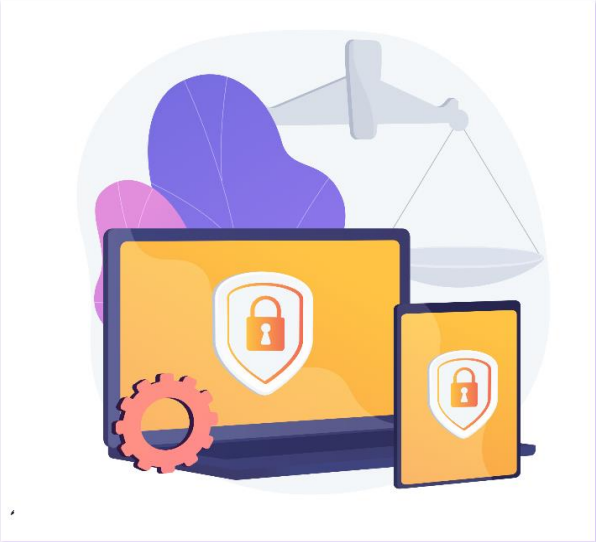
[43] Internet Matters, *Because children deserve a safe digital world*. Disponibil la: https://www.internetmatters.org/

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 digitali[44], 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%C5%9Fecul_Genera%C5%A3iei_Nativilor_Digitali_Document_de_pozitie.pdf

toate acestea, a ști cum să accesezi internetul pentru a intra în mediul online, nu este același lucru cu a-l folosi în siguranță. Ca părinți, nu trebuie să știți tot ce se petrece în lumea virtuală, dar, trebuie să aveți măcar cunoștințe minimale și să fiți pregătiți atunci când copiii întâmpină ceva necunoscut (nu neapărat și imediat evident ca fiind periculos pentru ei) sau nu sunt siguri cum să gestioneze o situație legată de e-mail sau despre potențialele riscuri prezentate de accesarea rețelelor sociale.

A-i asculta pe copii este extrem de important, deoarece creează premisele sănătoase ale unor îndrumări și sfaturi care să fie respectate de copii, fără efort și fără să genereze acestora un sentiment de apăsare, sau de presiune (“Trebuie să fac așa, pentru că așa mi-au cerut/impus părinții, deși eu vreau să fac altfel.”) și care să determine rezistența, sau chiar opoziția copiilor față de acestea (“Știu că părinții mei îmi vor binele/mă învață de bine, dar, ar fi putut să-mi permită să fac acest lucru măcar parțial, nu să-mi interzică complet. Las’ că găsesc eu o metodă să nu afle ce fac!”). Cel mai important lucru este să vă faceți copilul parte din conversație. Străduiți-vă să creați un mediu în care să poată pune întrebări în mod liber.

III.3. Ce trebuie să faceți când copiii accesează internetul?

Pentru început, utilizați instrumente de control parental. Profitați de această tehnologie care face posibilă blocarea site-urilor sau a categoriilor de pagini web care conțin material potențial dăunător pentru copii. Puteți filtra conținutul în funcție de vârsta copilului dvs.

Controlul parental poate fi folosit pentru a impune copiilor limite de timp pentru navigarea pe internet sau pentru jocuri - recomandarea noastră fiind să explicați copiilor de ce impuneți această limitare, să înțeleagă raționamentul din spatele acestor limite și să-i faceți să le accepte cât mai ușor, pentru a nu risca să obțineți efectul contrar așteptărilor dvs.

Soluțiile de control parental (ex: ESET[45] sau Family Link[46]) au și o funcție care le permite copiilor să solicite părinților acces la anumite pagini web, sau să ceară timp suplimentar de petrecut online. Din nou, acesta este un moment excelent pentru a discuta cu copilul despre menținerea sau relaxarea anumitor limite - adică să le explicați de ce le mențineți, sau care sunt condițiile în care ați fi dispuși să le relaxați.

Iată câteva sfaturi practice pentru părinți cu copii din diferite grupe de vârstă și care vor face mai sigure activitățile online ale acestora:

Până la 10 ani

- Însoțiți-i în primele lor călătorii digitale!

Stabiliți, ca prioritate, să fiți prezenți atunci când micuții dvs. fac primii pași în lumea digitală. Primul contact pe care îl are un copil cu internetul este un bun prilej de a-l ghida în noua lui aventură. Este, de asemenea, o șansă de a sublinia aspecte precum actualizările jocurilor, care ar putea necesita o achiziție și care ar trebui să fie autorizată de dvs., înainte de a fi efectuată.

- Stabiliți condițiile de utilizare a internetului

Setați regulile de bază pentru utilizarea internetului, inclusiv parametrii stabiliți/permiși de dvs. pentru jocurile online, pentru socializare sau pentru vizionarea de filme. O bună practică este

[45] ESET, *Parental control*. Disponibil după crearea unui cont personal, aici: https://parentalcontrol.eset.com/

[46] Google Family Link, Help keep your family safer online. Disponibil la: https://families.google.com/familylink/

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

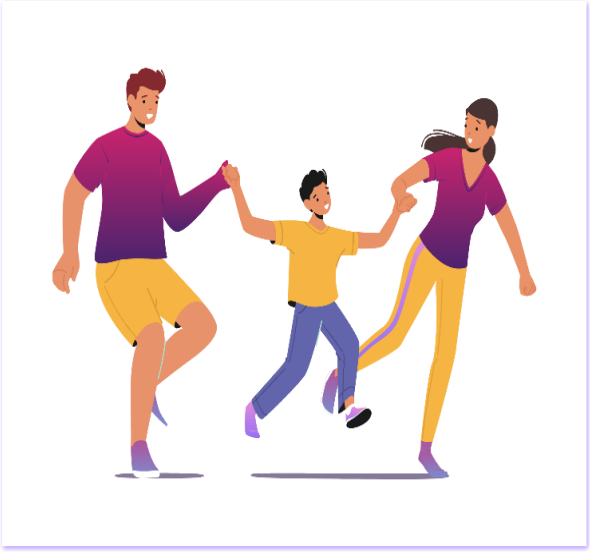
[47] Siguranța online. Disponibil la: https://sigurantaonline.ro/?fbclid=IwAR1UCwlo8DlaHfgzTDtyklb2AIWdtvNpVB2PYrvrFQi6zj8ieRUERSRmuzo

împărtășiți informații despre potențialele amenințări care pândesc pe rețelele sociale și pentru a vă oferi câteva soluții care vă vor ajuta să vă protejați familia.

Ce măsuri puteți lua pentru a vă proteja copiii pe rețelele sociale? Privind potențialele amenințări, utilizarea rețelelor sociale poate părea o activitate periculoasă. Cu toate acestea, interdicția de a le folosi nu va rezolva problema - copiii vor găsi o modalitate de a face ceea ce le place. În schimb, folosiți următoarele recomandări deoarece vă vor ajuta să faceți utilizarea rețelelor sociale mai sigură pentru copiii și familia dvs.:

- Păstrați permanent deschise canalele de comunicare cu copiii

Dialogul este una dintre cele mai importante componente pentru menținerea copiilor în siguranță în mediul online, mai ales când vorbim despre rețelele sociale. Menținerea unei comunicări deschise și sincere cu copiii dvs. este importantă, dacă vreți ca aceștia să aibă încredere în judecata dvs. și să vă urmeze sfaturile. Un bun exemplu este cyberbullying-ul și prevenirea acestuia. Spuneți-i clar copilului că hărțuirea cibernetică este complet inacceptabilă, indiferent dacă sunt ei înșiși vizați sau dacă sunt tentați să participe la atacarea altora.



Când se confruntă cu un astfel de comportament, chiar dacă nu îi privește în mod direct, ar trebui să anunțe imediat pe cineva - pe dvs., un profesor sau alți adulți responsabili.

- Utilizați aplicații de control parental

În funcție de vârsta copiilor dvs., puteți utiliza software-ul de control parental pentru a seta o listă de site-uri web sau aplicații blocate și pentru a restricționa orele la care copilul dvs. poate fi prezent online. De asemenea, puteți oferi copilului dvs. acces complet la tot ce este online, cu monitorizare încorporată, care vă permite să vedeți ceea ce vede copilul.

Copilul dvs. ar trebui să facă parte din procesul de luare a deciziilor. Dacă alegeți să le limitați accesul sau timpul online, software-urile de control parental le permit copiilor să vă solicite, în timp real, permisiunea de a vizita anumite site-uri web sau de a beneficia de timp suplimentar petrecut pe rețelele sociale. Amintiți-vă: doriți să încurajați discuțiile despre importanța echilibrării timpului petrecut pentru socializare online cu alte obligații ale copiilor, cum ar fi efectuarea temelor pentru acasă.

- Utilizați protecția anti-spam și firewall

Este recomandată instalarea pe dispozitivele copilului dvs. a unei soluții de securitate cu capacități de detectare proactivă, pentru a evita programele malware[48], ransomware[49], tentativele de phishing etc., atunci când utilizați rețelele sociale. Asigurați-vă că soluția pe care o alegeți include protecție antispam și firewall.

- Utilizați parole puternice și verificarea în doi factori

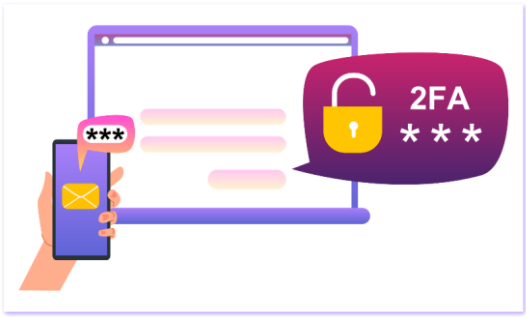
[48] Cisco, *What is malware?* Disponibil la:

https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html#tabs-35d568e0ff-item-194f491212-tab

[49] Wikipedia, Ransomware: "este un software rău intenționat care, după ce se instalează pe dispozitivul victimei (calculator, smartphone), criptează datele victimei ținându-le „ostatice", sau șantajează victima, pe care o amenință că îi va publica datele dacă aceasta nu plătește o „răscumpărare" (în engleză "ransom"). De cele mai multe ori, ransomware-ul păcălește victima, spunându-i că s-a găsit activitate ilegală pe dispozitiv și că trebuie să plătească o sumă de bani ca să recapete controlul asupra dispozitivului. Disponibil la:

https://ro.wikipedia.org/wiki/Ransomware#:~:text=Ransomware%20este%20un%20software%20r%C4%83u,%E2%80%9D%20(%C3%AEn%20englez%C4%83%20ransom).

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 agreseze cibernetic sau chiar să încerce să-i fure identitatea.

- Schimbați setările profilului în “mod privat”

Setările implicite de confidențialitate pentru rețelele sociale nu vor garanta siguranța copilului dvs. Pentru început, profilurile ar trebui să fie setate pe opțiunea “privat” în loc de “public”. Pentru exemplificare, vom folosi platforma Instagram și un telefon mobil: conectați-vă la profilul copilului dvs. atingând pictograma “persoană”. Glisați spre stânga și atingeți pictograma “Setări” (de obicei, pictograma respectivă este o rotiță dințată). Selectați “Confidențialitate și securitate”, apoi “Confidențialitatea contului”, după care activați “Contul privat”.

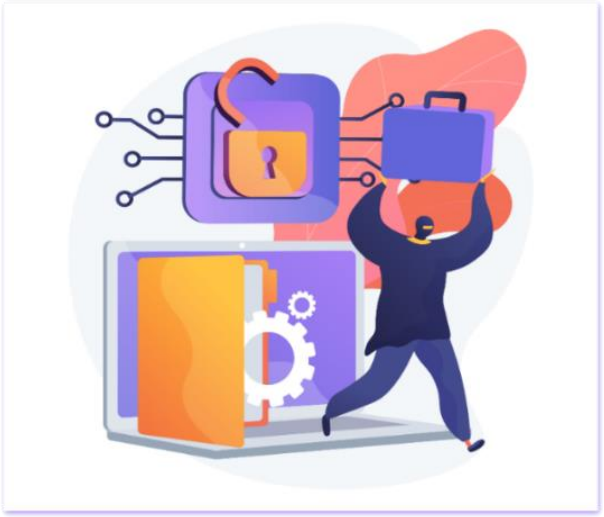
- Câteva recomandări pentru utilizarea în siguranță a rețelelor sociale

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.

8. Învățați copilul să folosească webcam-ul pentru a comunica exclusiv cu oameni pe care îi cunoașteți și dvs. în viața reală și să închidă camera atunci când nu o folosește.
9. Învățați copilul să nu pună în circulație mesaje vulgare, imagini sau alte materiale cu el sau cu alți cunoscuți în ipostaze indecente.
10. Învățați copilul să nu răspundă la mesaje menite să-l hărțuiască, și să blocheze expeditorii unor astfel de mesaje.
11. Învățați copilul cum să respingă și să blocheze mesaje sau contacte nedorite.
12. Învățați copilul să se deconecteze de la internet, atunci când nu îl folosește.

- Recomandări pentru părinți

1. Discutați constant cu copilul despre comportamentul acestuia în mediul online.
2. Aflați exact ce -site-uri de socializare folosește copilul, pe cine are în lista de prieteni (repetați, împreună cu el, recomandările noastre de mai sus).
3. Folosiți firewall-ul și alte programe de securitate online pentru a bloca site-urile cu conținut neadecvat pentru copii.
4. Monitorizați activitatea online a copilului (restricționați accesul la programe, softuri și site-uri care i-ar putea face rău).[50]



III.5. Care sunt principalele amenințări online?

Programele de tip malware (software rău intenționat)

Acestea sunt proiectate să deterioreze sau să blocheze dispozitivul, să fure datele sau să le răspândească în alte rețele. Diferite tipuri de programe malware vă pot cripta fișierele și le pot păstra pentru răscumpărare, pot încerca să vă acceseze informațiile financiare, să vă spioneze activitățile prin intermediul camerei web și multe altele. Pe lângă utilizarea unei soluții fiabile de securitate pe internet, educați copiii despre amenințările de pe internet și cum puteți să le evitați împreună. O resursă excelentă de informații, avertismente și recomandări de prevenire a unor asemenea situații, atât pentru copii, cât și pentru adulți, este site-ul Directoratului Național de Securitate Cibernetică (DNSC).[51]

Spam

Ați mai văzut spam, sub forma tuturor acelor e-mail-uri nedorite și nesolicitate care apar în căsuța dvs. de e-mail. Ar trebui șterse, fără a le deschide. Amintiți-le copiilor că aceste mesaje nedorite încearcă, adesea, să vă atragă către site-uri web sau anunțuri concepute pentru a răspândi programe malware, pretinzând că ați câștigat un concurs sau oferind produse „gratuite”.

Înșelătorii

Înșelătoriile pe internet pot lua mai multe forme, cum ar fi spam-ul și utilizarea tehnicilor de inginerie socială. În cea din urmă, escrocul poate pretinde că este un coleg de școală sau un profesor, pentru a încerca să colecteze informații confidențiale, cum ar fi Codul Numeric Personal (CNP), nume de utilizator și parole. E-mail-urile sau textele care solicită nume de utilizator și parole pentru rețelele sociale sunt alte înșelătorii comune.

Cyberbullying

[50] *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

[51] Directoratul Național de Securitate Cibernetică: https://dnsc.ro/

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?

6. Cât de des vorbiți cu copilul despre lumea digitală, și, mai ales, despre lumea lui digitală?

Poate ați auzit sau ați fost martor al unor situații ca cele enumerate în continuare:

- „Copilul meu este hărțuit pe Facebook, am fost victima unui atac de phishing, colega mea a fost concediată pentru anumite postări pe rețelele sociale, am primit mesaje de la necunoscuți care mă amenințau cu postarea unor filmulețe care mă puneau într-o lumină nefavorabilă”… și lista poate continua.

Trăim într-o perioadă în care o mare parte din viața noastră, personală și profesională, s-a mutat în mediul online. Această dependență crescută de internet și de rețelele digitale aduce și riscuri împreună cu confortul oferit.

O primă modalitate importantă și foarte utilă pentru a educa și gestiona securitatea digitală a copiilor, pe termen scurt, mediu și lung, este COMUNICAREA cu aceștia.

- În calitate de părinte, sunteți cea mai bună protecție a copilului împotriva amenințărilor online. Ca să îl determinați să înțeleagă la ce este expus, puteți începe cu o întrebare simplă: „Tu știi cât de extinsă este amprenta ta digitală?” Tastați-vă numele sau numele copilului pe Google Search și observați rezultatele... Și acesta e locul cel mai transparent de unde puteți afla acest lucru.
- Amprenta digitală cuprinde tot ce s-a postat vreodată pe internet: fotografii, înregistrări audio, videoclipuri, texte, like-uri și comentarii. Toate acestea arată cine este persoana pe internet și reprezintă amprenta sa digitală.
- Ca în multe alte situații, comunicarea efectivă poate fi soluția. Da, poate fi dificilă, dar nu renunțați! Stați de vorbă cu copilul dvs. și nu subestimați niciodată valoarea comunicării față în față!
- Fiți deschiși la a discuta cu copiii dvs. despre tehnologie și activitatea pe internet. Are un puternic impact să îi spuneți copilului: „Dacă ai o problemă pe internet, sau chiar dacă greșești, vreau să vorbești cu mine despre asta și promit că voi face tot ce pot să te ajut să rezolvi problema, astfel încât să poți învăța și să te poți distra în continuare în online”.
- Menținerea comunicării cu copilul este importantă pentru a vă asigura că timpul petrecut online este distractiv și sigur. Punând întrebări atent formulate, puteți obține o imagine a modului în care copilul folosește tehnologia și cum îl puteți ajuta să o gestioneze mai bine.
- Este o idee bună să începeți prin a întreba copilul despre activitatea prietenilor lui pe internet, deoarece nu se simte direct vizat și este mai puțin reticent în a răspunde.

Exemple de întrebări pe care le puteți adresa copilului:

- Prietenii tăi folosesc computerul?
- Ce fac ei pe computer?
- Ce jocuri jucați împreună?

Odată ce ați stabilit o legătură, profitați de ocazie pentru a pune întrebări generale și apoi solicitați clarificări atunci când este nevoie. Unele dintre aceste întrebări pot fi:

- 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 greșeală, 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 dependența de internet*. Disponibil la: https://www.winddiscovery.ro/blog/tratare-dependenta-calculator/

Încearcă să ascundă ceea ce face:

- Nu partajează parolele cu unul dintre părinți;
- Încuie ușa de la camera sa;
- Oprește brusc ceea ce face pe telefon/laptop/consolă, la vederea părinților.

Devine mai retras:

- Nu vrea să vorbească despre internet, tehnologie;
- În istoricul browser-ului observați că a accesat un site neobișnuit;
- Identificați vizite suspecte ale unor site-uri sau cuvinte de căutare care vă ridică semne de întrebare (da, puteți și ar trebui să verificați periodic istoricul de navigare al copilului dvs.).

Schimbări:

- Vorbește despre noi „prieteni" din online;
- Folosește un limbaj neobișnuit pentru vârsta lui (înjurături, conotații sexuale);
- Pune întrebări despre lucruri sau subiecte care par neobișnuite/neașteptate;
- Are coșmaruri, prezintă modificări ale comportamentului (cel mai adesea devine semnificativ mai retras decât de obicei, mai agresiv etc.);
- Dă semne de oboseală neobișnuită (un semn că se strecoară pe timp de noapte la joacă);
- Suferă de dureri de cap (de la o postură greșită la calculator);
- Pierde în mod regulat mesele (nu doar accidental), pentru a rămâne la calculator.

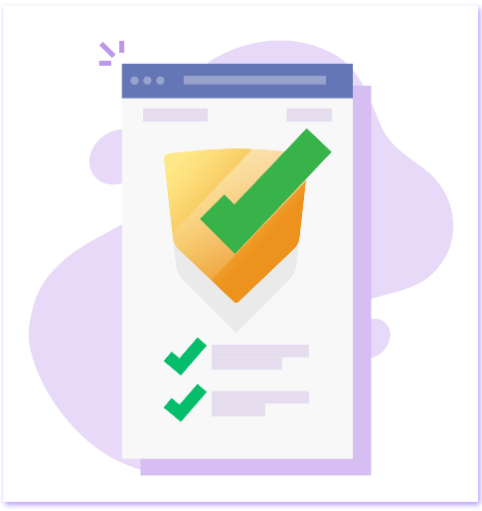
Încercați să fiți prezent în lumea digitală a copilului! Observați copilul și găsiți timp pentru a vorbi cu acesta despre constatările și suspiciunile pe care le aveți.

Nu trebuie să treceți singur prin asta!

- Înconjurați-vă cu o rețea de oameni de încredere cu care puteți face schimb de informații (diriginte, învățător, profesori, alți părinți, prieteni de familie care au aceleași probleme, specialiști etc.). Dacă vă simțiți încrezător în capacitățile dvs. și nu vă lăsați timorat de noua tehnologie, puteți crea o experiență online sigură și distractivă pentru copilul dvs.
- Când sunteți pregătit și normalizați discuțiile cu alți adulți despre interacțiunea cu noua tehnologie, trăiți, mai degrabă, un sentiment de sprijin și de suport, decât de izolare. Aflați cu ce se confruntă și alți părinți, vedeți lucrurile și din altă perspectivă. Puteți afla lucruri care se pot întâmpla online, despre care nu erați conștienți. Învățăm unii de la alții.

III.7. Controlul parental - Gestionarea dispozitivelor (o problemă delicată)

Părinții ar trebui să folosească programe sau aplicații pentru a **monitoriza activitatea online a copiilor**. Familiile care au avut probleme cu mediul online au spus că ar folosi, acum, monitorizarea sau software-ul de filtrare, dacă ar putea da timpul înapoi și ar putea detecta, din timp, o potențială problemă.



Dacă părinții încep să folosească devreme programele de monitorizare sau filtrare, acestea vor deveni parte din lumea online a copilului. Se vor obișnui să fie folosite acasă, așa cum se pot aștepta să le întâlnească la școală și, apoi, la locul de muncă. Nu discutăm aici și acum dacă suntem pro sau contra, părerile pot fi împărțite. Dar este o soluție utilă pentru perioada când copiii sunt mai mici și e nevoie de mai mult control parental, sub toate formele lui.

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.

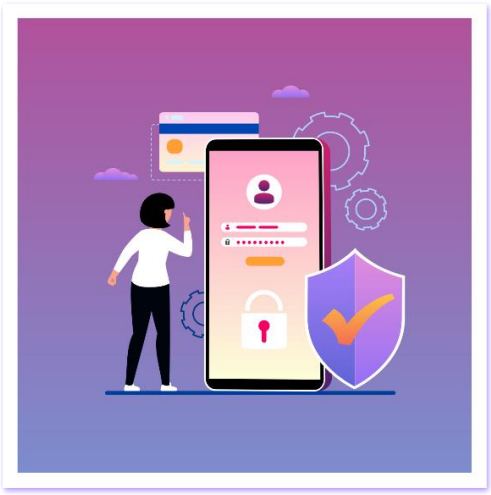
Prețuiți datele personale ale copilului!

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 colectorii 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

comportament online responsabil, inclusiv să se gândească la impactul postării unei fotografii sau al unui comentariu.

Amintiți-le că nu este întotdeauna ușor să retragi ceva ce ai postat online și că textele și fotografiile pot fi redirecționate oricui. Este bine să învățați copiii regula de aur conform căreia lucrurile pe care nu le-ar face în viața reală nu ar trebui făcute nici online.

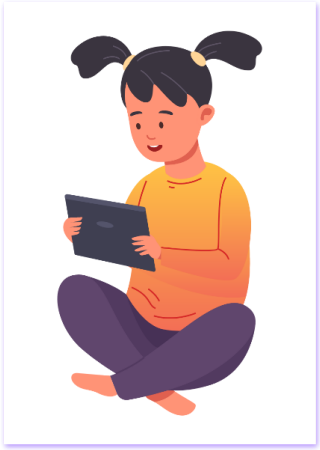
Învățați-i cum să raporteze comportamentul răutăcios sau conținutul neplăcut de pe site-urile lor preferate!

Fiți la curent și țineți pasul cu noile modalități de a rămâne în siguranță online și cu modalitățile de a gestiona confidențialitatea!

Continuați să discutați cu copiii, nu doar pentru a-i învăța, ci și pentru a învăța de la ei. Probabil că știu mai multe decât dvs. despre ceea ce este în online!

Utilizați aplicații pentru control parental!

Îndrumați-vă copilul către conținutul potrivit! Este ușor să aflați cât timp petrece copilul dvs. pe aplicațiile preferate din rapoartele de activitate ale aplicației de control parental. Dacă simțiți că petrece prea mult timp pe o anumită aplicație, puteți seta limite de timp de utilizare pentru fiecare aplicație, sau dacă doriți ca acesta să ia o pauză de la utilizarea unei aplicații, puteți să ascundeți aplicația astfel încât să nu mai fie accesibilă pe dispozitivul copilului. De asemenea, îl puteți încuraja să folosească anumite aplicații mai des, adăugându-le la o listă de aplicații care sunt întotdeauna permise.



Urmăriți timpul petrecut în fața ecranului/cu ochii pe display! Setați o limită zilnică de timp pentru a vă asigura că nu petrece prea mult timp în fața dispozitivelor/în online. Dacă bănuiți că există situații în care copilul dvs. stă treaz până târziu, "cu ochii în ecran", puteți seta și o oră de "culcare" a acestuia, care îi va bloca telefonul până dimineață. Acest lucru vă va ajuta să vă asigurați că dispozitivul nu le perturbă somnul și rutina.

Ajutați-i să lase telefonul din mână! Fie că este ora cinei, este timpul să termine temele sau, poate, doar timpul să ia o pauză de la privitul în ecran, puteți bloca oricând dispozitivul copilului dvs., de la distanță. Acest lucru îi va ajuta să înțeleagă că este timpul să se deconecteze și să se concentreze pe altceva decât pe ecrane.[54]

Stabiliți reguli și limite - "Regulile casei" pentru securitate digitală!

Și părinții și copiii au nevoie de reguli și limite (la serviciu, la școală, la restaurant, la cinema, la muzeu, în sala de sport - ca să dăm doar câteva exemple). Regulile nu-i opresc să se distreze și să învețe, ci îi protejează. Dar, părinții trebuie să fie și flexibili, regulile pot fi schimbate, dacă se constată că nu sunt potrivite.

Regulile generale pot include:

- Limite de timp și restricții (o modalitate de avertizare pentru depășirea limitei de timp);
- Înțelegere a limbajului acceptat și acceptabil;
- Stabilirea locurilor din casă în care tehnologia poate sau nu poate fi utilizată;
- Ce pagini web, jocuri și aplicații pot fi accesate/utilizate;
- Ce trebuie să faceți dacă se întâmplă ceva îngrijorător sau se face o greșeală;
- Acestea nu sunt opționale: Fiți ferm… dar flexibil.

Reguli și limite pentru timp și parole:

[54] *Tips for Family Link from Google*. Disponibil la: https://services.google.com/fh/files/misc/google_families_familylinktips.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 protejez parolele;
  - Nu împărtășesc parola mea nimănui, cu excepția părinților;
  - Măcar unul dintre părinții mei are parolele mele pentru orice dispozitiv sau site web.

Iată 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

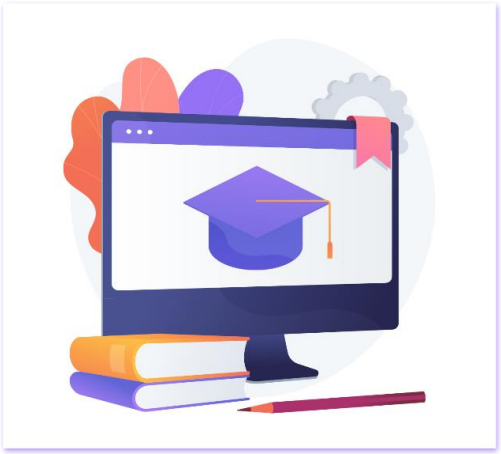
NOTĂ * Pentru setarea subtitrării în limba romană pe https://www.youtube.com/ alegeți din setări **“Subtitles”** (subtitrări) și apoi alegeți **limba română** din listă.

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

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

care nu au existat niciodată înainte, inclusiv schițe și editări care sunt înregistrate și arată ritmul și evoluția performanței lor școlare. Comunicări între elevi și profesori, sau între elevi - de la temele de matematică până la metadatele comportamentului lor online în timp ce utilizează o aplicație - sunt acum create, colectate, și adesea prelucrate de furnizori terți de tehnologie educațională.

Dumneavoastră, profesorii trebuie să utilizați bunele practici digitale și comportamentale cu elevii dumneavoastră. Aceasta include atenția sporită la produsele digitale și procesele care sunt încorporate în orice proiect sau design de lecție online.

IV.2. Ce înseamnă date personale ale elevilor?

Informațiile care sunt legate de elevi sunt denumite date cu caracter personal și sunt supuse unor restricții suplimentare din punct de vedere legal, mai ales în cazul serviciilor informaționale oferite minorilor sub 16 ani. Datele personale ale elevilor includ orice informații despre identitatea unui elev, studiile sale, condițiile medicale sau orice altceva care este colectat, stocat și comunicat de școli sau furnizori de tehnologie în numele școlilor, care este specific pentru acel elev. Acestea includ numele, adresa, numele părinților sau tutorilor, data nașterii, profilul educațional, prezența, dosarele disciplinare, notele sau calificativele, nevoile speciale și alte informații necesare pentru administrarea și instruirea de bază. Includ, de asemenea, datele create sau generate de elev sau profesor în utilizarea tehnologiei - conturi de e-mail, munca efectuată cu un program sau aplicație educațională, orice altă informație despre elev în cadrul educațional.

IV.3. Aplicațiile și platformele educaționale

Ce faceți dacă doriți să folosiți o aplicație sau un instrument educațional și nu știți dacă școala/inspectoratul/ministerul le-a verificat și aprobat?

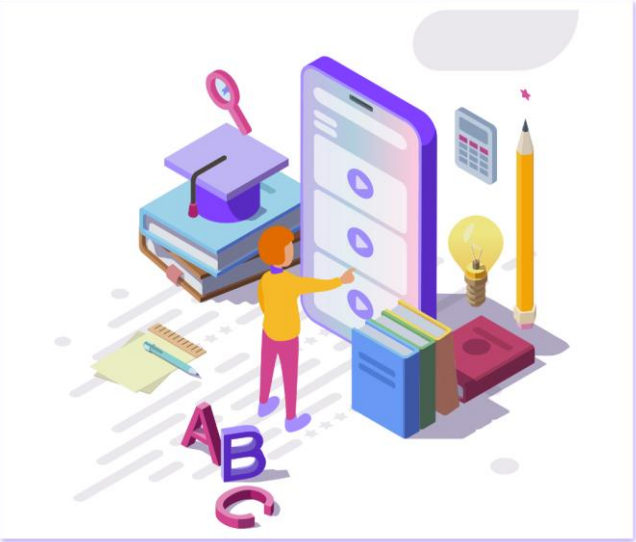
Ca profesori, familiarizați-vă cu politica sau procesul școlii dvs. de selectare a noilor instrumente educaționale, dacă există. Atunci când o aplicație sau un serviciu pe care doriți să le utilizați nu se află pe lista „aprobată”, solicitați verificarea acesteia și întrebați cât timp durează procesul de verificare. Dacă procesul este lung, va trebui să vă regândiți lecția sau temele. Odată ce aplicația este aprobată, cu siguranță o puteți utiliza mai târziu. Lista poate conține, de asemenea, aplicații alternative similare pe care le puteți utiliza între timp.

Dacă școala are o listă aprobată de produse, servicii, site-uri sau aplicații tehnologice, verificați dacă serviciul pe care îl utilizați este inclus și asigurați-vă că sunteți la curent cu cerințele sau opțiunile de confidențialitate care sunt agreate. Atunci când școlile decid să folosească anumite instrumente tehnologice, ar trebui să evalueze acele instrumente pentru a se asigura că îndeplinesc cerințele privind confidențialitatea/protecția datelor personale.

Câteva exemple de astfel de instrumente includ:

- Un flux de lucru și instrumente de învățare în care/cu care elevii și profesorii lucrează împreună, oferă feedback și comunică pe parcursul procesului de învățare;
- Un sistem de lucru în care profesorii postează instrucțiuni, sarcini și link-uri către resurse pe care elevii și părinții le pot accesa.
- Cataloagele online, în care profesorii postează note, iar elevii și părinții le pot accesa, folosind un nume de utilizator și o parolă.
- Instrumente de comunicare pentru e-mail-uri sau notificări tip newsletter.

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

școli să nu aibă politicile de confidențialitate adaptate pentru a asigura protecția datelor utilizatorilor.

Prin urmare, dacă nu sunt interzise de politica școlii, aceste produse ar trebui evaluate cu atenție pentru a vedea dacă utilizarea lor este conformă cu legislația privind protecția datelor personale. Dacă un elev vă cere să utilizați pentru temă o aplicație pe care nu o cunoașteți, este o idee bună să folosiți ocazia pentru a vorbi cu elevul dvs., folosind întrebările sugerate mai sus.[57]

IV.4. Provocările Educației Online – cu ce ne putem confrunta?

Lumea digitală are și părți bune și nu trebuie blamată pentru părțile ei mai puțin bune, deoarece trebuie să fim conștienți că orice prezintă riscuri, indiferent dacă se manifestă în viața reală, fizică, palpabilă, sau doar în mediul online. Noi suntem cei care trebuie să învățăm să ne adaptăm, să ne protejăm, să ne educăm continuu și să conștientizăm riscurile cu care ne confruntăm.

În calitate de profesor, trebuie să fiți informat și să vă însușiți cele mai bune practici pentru a vă proteja pe dvs. și pe elevi. Iată doar două exemple:

- Phishing: Aceste atacuri valorifică ingineria socială prin exploatarea emoțiilor umane, pentru a păcăli victimele să divulge informații sensibile, cum ar fi parolele sau detaliile cardului bancar. Peste 90% dintre atacurile cibernetice de astăzi încep cu phishing, potrivit CoSN (Consorțiul pentru rețelele școlare S.U.A.)
- Vulnerabilități IoT: Dispozitivele IoT (Internetul lucrurilor – Internet of Things), cum ar fi televizoarele SMART, accesoriile pentru casa inteligentă și tabletele, adesea nu sunt securizate, sau mijloacele de protejare a acestora nu sunt actualizate în mod regulat. Este, deci, important ca profesorii să acorde prioritate securității cibernetice, atunci când includ dispozitive IoT în sala de clasă sau în educația online.

Sunteți pregătiți să faceți față noilor provocări?

O mare parte a problemei, la nivel mondial, este lipsa de conștientizare și de instruire în rândul dascălilor, a personalului auxiliar din școli și a elevilor, cu privire la riscurile mediului online și la mijloacele de prevenire a acestora sau de protecție, în general – ”plecați la război fără arme și fără să vă cunoașteți inamicul.”

Așa cum am mai spus, securitatea cibernetică este un sport de echipă. Colaborarea este cheia – creați o mentalitate de siguranță digitală pentru toți cei implicați! Ca profesor, vocea dvs. are greutate – și nu doar în sala de clasă!

Nu toate amenințările digitale provin din afara școlii. Orice politică serioasă de siguranță cibernetică trebuie, de asemenea, să abordeze problemele care pot apărea chiar și de la elevi. Pentru început, ar trebui să fiți conștienți de provocările și oportunitățile practice ale lucrului cu tinerii care au crescut cu tehnologia modernă. Așa cum propriii noștri profesori au păstrat lucrările de examen închise în siguranță într-un sertar de birou, va trebui să luați măsuri similare pentru a împiedica elevii să vă acceseze datele și să trișeze, sau să-și schimbe notele, de exemplu.

Deoarece sunteți în prima linie de apărare atunci când vine vorba de a proteja școlile de amenințările cibernetice, este logic să vă folosiți vocea pentru a susține o mai bună securitate digitală, precum și politici mai cuprinzătoare. Puteți implica părinții într-un dialog, împărtășindu-

[57] ConnectSafely, Kerry Gallagher, Larry Magid, and Kobie Pruitt, *The Educator's Guide To Student Data Privacy*. Disponibil pentru download direct, la: https://www.connectsafely.org/wp-content/uploads/Educators-Guide-Data-.pdf

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

- Dumneavoastră, Profesorul, trebuie să-i învățați pe copii ce este (cyber)bulling-ul, care sunt limitele dintre distracție și (cyber)bullying și cum să reducă riscul de (cyber)bullying.
- Trebuie să-i sfătuiți cum să procedeze dacă se confruntă cu hărțuirea în mediul on-line. Recomandați-le anumite persoane la care pot apela dacă întâmpină probleme, cum ar fi părinții lor, un frate mai mare sau un coleg pentru sprijin emoțional sau un profesor pentru suport tehnic. Învățați copiii cum să procedeze atunci când li se întâmplă ceva rău pe internet.

- Îmbunătățiți abilitățile sociale ale copiilor, încurajați empatia. Îi puteți ajuta pe copii învățându-i să-și distingă propriile sentimente, astfel încât să fie mai sensibili la propriile experiențe și la experiențele altora. De asemenea, îi puteți ajuta să-și îmbunătățească percepția de sine și abilitățile sociale, astfel încât să poată construi și menține relații sănătoase cu ceilalți. În cadrul clasei, puteți susține valori precum prietenia, acceptarea și apartenența la un grup.
- Încurajați copiii să-i ajute pe cei care sunt mai slabi. Dezvoltați-le copiilor capacitatea de a se apăra activ pe ei înșiși și pe alții, dacă cineva îi rănește.
- Dezvoltați abilitățile copiilor de utilizare a internetului în siguranță. Puteți explica elevilor cum să se protejeze mai bine, folosind mijloacele tehnice disponibile.
- Creați locuri și zone sigure pe internet pentru victimă. Puteți ajuta la crearea unor zone sigure, în care copiii agresați pot opera fără să se teamă de atacuri ulterioare.
- Asigurați elevii că este bine să se încreadă în adulții din jurul lor. Le puteți explica elevilor că este important ca adulții în care au încredere să cunoască problema cu care se confruntă. Dacă nu au cunoștință despre această problemă, adulții nu pot oferi ajutor.

Cum ar trebui să reacționați când un copil vă spune că este agresat?

Cum se procedează în ceea ce privește victima:

- Elevul are nevoie de ajutorul unei persoane care oferă sprijin social și este calificată să rezolve incidentul. Pe lângă acordarea de sprijin emoțional, ascultarea și ajutarea copilului să-și exprime sentimentele, le puteți explica și ce trebuie să facă în continuare:
  - Păstrați dovada agresiunii, cum ar fi mesaje SMS, mesaje de pe chat, fotografii umilitoare, comentarii sau capturi de ecran ale aplicațiilor online. Acesta este un pas important, deoarece copilul poate și este de înțeles ca ar dori să șteargă conținutul nepotrivit, pentru a preveni răspândirea acestuia. Cu toate acestea, tocmai acest conținut este dovada necesară pentru a lua măsuri împotriva agresorului.
  - Nu comunicați cu agresorul, blocați-l și eliminați-l din contacte. În acest moment, agresiunea se poate opri. Totuși, este necesar să-l ajutăm pe copil să rezolve orice conflicte existente și să mențină relații funcționale cu semenii săi.

Cum se procedează în ceea ce privește școala, părinții, profesioniștii și autoritățile:

- Nu trebuie să treceți cu vederea sau să ascundeți informații despre relele tratamente între elevi, deoarece acestea reprezintă o încălcare a drepturilor copilului. În cazuri similare, contactați întotdeauna conducerea școlii și reprezentanții legali ai elevului afectat.
- Acționați imediat și încercați să ajutați elevul, în colaborare cu alte persoane relevante din sistemul școlar, adică părinții, elevul însuși, colegii de clasă, directorul, alți profesioniști ai școlii, cum ar fi psihologul școlar sau poliția.

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.
- Ajutați 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.
- Ajutați 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 educațional[60], 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

Măsurile ar trebui să fie specifice circumstanțelor prelucrării și riscurilor prezentate pentru copii și vizează asigurarea confidențialității, integrității, disponibilității, autenticității datelor copiilor în orice context în care sunt prelucrate, precum și a rezistenței sistemelor și serviciilor de prelucrare.

Prin urmare, evaluarea riscurilor ar trebui să urmărească obținerea de rezultate care să includă standarde înalte de securitate pe parcursul procesării, ținând cont de natura, domeniul de aplicare, contextul și scopurile acesteia, precum și de riscurile pe care le prezintă. O astfel de evaluare trebuie să fie bazată pe considerente de necesitate și proporționalitate, precum și de principiile fundamentale de protecție a datelor:

- în gama de riscuri, inclusiv accesibilitatea fizică;
- acces în rețea la dispozitive și date;
- backup și arhivare a datelor.

Accesibilitatea fizică (de exemplu, la dispozitive și date din mediul educațional) include date colectate sau stocate în cel puțin următoarele contexte:

- clasă/învățare electronică (inclusiv învățământ la distanță în afara școlii);
- administrația școlii;
- spații (acces fizic, CCTV inclusiv pe vehiculele școlare, cititoare biometrice).

Trebuie să se ia în considerare modul în care utilizatorii copii ar trebui să se autentifice la sisteme, inclusiv dacă acest lucru este necesar în contextul prelucrării. Când evaluăm riscurile, trebuie să luăm în considerare cum se face autentificarea pentru orice sistem pe care îl folosim. Este important să alegem metode de autentificare care protejează confidențialitatea utilizatorilor.

De exemplu, în loc să folosim nume de utilizator și parole care pot fi ușor asociate cu o persoană, putem folosi alte metode cum ar fi token-uri. Autentificarea ar trebui să fie robustă și capabilă să garanteze că datele sunt protejate. Principiile limitării scopului și minimizării datelor ar trebui, de asemenea, să facă parte din evaluarea oricărui sistem de autentificare.

Pentru accesul la date, în rețea, autentificarea este necesară pentru a preveni accesul neautorizat. Apar aceleași întrebări ca și în cazul accesului la fața locului: care este cea mai potrivită tehnologie de autentificare și este accesul acordat pe baza identității individuale (prenume, nume) sau a unui atribut („elev la această școală”)?

Evaluarea riscurilor înainte de prelucrare trebuie, de asemenea, să aprecieze dacă datele sunt protejate împotriva accesului, modificării și eliminării sau distrugerii neautorizate. În cazul în care datele sunt prelucrate în afara amplasamentului (de exemplu, de către terți furnizori de servicii), furnizorii de educație trebuie să rămână conștienți de responsabilitățile lor permanente în calitate de operatori de date. Trebuie făcut efortul necesar pentru a stabili capacitatea terțului de a proteja datele cu caracter personal în mod corespunzător, inclusiv confidențialitatea, integritatea și disponibilitatea.

Întrebări similare ar trebui puse în legătură cu datele digitale care sunt stocate în scopuri de backup și/sau de arhivare, mai ales dacă aceste servicii sunt furnizate de terți - fie în mod explicit (cum ar fi pentru un serviciu de arhivare contractat), fie implicit, ca parte a disponibilității datelor.

Pot fi aplicate (și chiar combinate) numeroase niveluri de protecție. Datele criptate ar trebui gestionate într-un mod similar cu datele de backup/arhivare. Adică, procesul de recuperare a datelor ar trebui testat în mod regulat.

Orice măsuri puse în aplicare ar trebui să fie testate în mod regulat și să se ia în considerare metodele și tehnicile și riscurile de securitate a datelor și să fie monitorizate periodic și actualizate acolo unde este necesar.

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 dispare. 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 frauda 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 frauda 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://dnsc.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://dnsc.ro/vezi/document/ce-fac-daca-mi-s-au-furat-datele-de-card-sau-de-date-bancare

4. Actualizează software-ul antivirus pentru a fi apărat de orice nou virus informatic și pentru a proteja dispozitivul folosit.
5. Anunță Poliția despre problemă, dacă ți s-au extras bani din cont.
6. Semnalează frauda către DNSC.
7. Păstrează orice posibilă dovadă a escrocheriei, de exemplu, e-mailuri, facturi, chitanțe, copii ale reclamei etc.
8. Vorbește cu familia și prietenii despre acest incident, ajutându-i, astfel, să fie pregătiți pentru această metodă de atac.[63]

Ce este DNSC și cum poate fi contactat?

Directoratul Național de Securitate Cibernetică (DNSC) este autoritatea civilă de securitate cibernetică a României, unde un utilizator poate raporta incidente sau suspiciuni de incidente de securitate cibernetică, fie prin e-mail, la: alerts@dnsc.ro, fie la numărul de urgență dedicat incidentelor de securitate cibernetică, 1911, unde un utilizator poate discuta direct cu un operator specializat despre problema sa.[64] În multe cazuri, utilizatorii sunt panicați și nu știu clar ce să facă, cui să se adreseze, iar, de multe ori, viteza de reacție poate fi vitală. Consultați cu periodicitate site-ul www.dnsc.ro pentru a fi la curent cu noutățile despre incidentele de securitate cibernetică, alerte, amenințări cibernetice etc.

Recomandăm, totodată, campania de prevenire a criminalității informatice în rândul tinerilor ale cărei detalii le puteți găsi aici: Campanie de prevenire a criminalității informatice în rândul tinerilor (dnsc.ro).[65]

O resursă importantă pentru copii, părinți și profesori este site-ul campaniei Siguranța online[66], proiect de conștientizare la nivel național, dedicat tuturor utilizatorilor, inițiat de DNSC, Poliția Română și Asociația Română a Băncilor. Site-ul sigurantaonline.ro este un instrument util pe care un utilizator obișnuit îl poate utiliza pentru a deprinde o serie de reflexe vitale pentru protecția în mediu online. Acest site are totodată și o componentă dedicată copiilor, care include testarea abilităților de securitate cibernetică ale acestora, dar și mai multe broșuri cu benzi desenate, prin intermediul cărora li se explică copiilor cum funcționează principalele amenințări din mediul online. Broșurile pot fi descărcate gratuit de pe site.[67]

[63] DNSC, *Ați fost păcălit printr-un scam?* Disponibil pentru download direct, la: https://dnsc.ro/vezi/document/cum-procedez-daca-am-fost-pacalit-printr-un-scam

[64] DNSC, Our contact information, https://dnsc.ro/contact

[65] DNSC, *Campanie de prevenire a criminalității informatice în rândul tinerilor*. Disponibil la: https://dnsc.ro/pagini/campania-prevenire-criminalitate-informatica

[66] https://sigurantaonline.ro/

[67] Siguranța online, POVEȘTI, Disponibil la: https://sigurantaonline.ro/povesti/

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.certsign.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.htp_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:[1]}
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:

https://www.youtube.com/watch?v=affu-bFKdeM&t=12s
24.Cyber4Kids. Cyberbullying. Disponibil la:
https://www.youtube.com/watch?v=686eAFXTW5A&t=6s
25.Cyber4Kids. Parole magice. Disponibil la:
https://www.youtube.com/watch?v=F4iTwb-3SBY&t=61s
26.Cyber4Kids. Secret personal data. Disponibil la:
https://www.youtube.com/watch?v=0BNr9bIgAzY&t=36s
27.Cyber4Kids. The Internet never forgets. Disponibil la:
https://www.youtube.com/watch?v=nINV6bLM_9M&t=16s
28.Cyber4Kids. Welcome to Cyber City! Disponibil la:
https://www.youtube.com/watch?v=ldYHVhi4GUQ
29.Cyber4Kids. We play safely. Disponibil la:
https://www.youtube.com/watch?v=Irobrzu9qwU
30.Cyber4Kids. WiFi sau nu? Disponibil la:
https://www.youtube.com/watch?v=OKtbTTv3fvg&t=98s
31.DNSC, Ați fost păcălit printr-un scam? Disponibil pentru download direct, la: https://dnsc.ro/vezi/document/cum-procedez-daca-am-fost-pacalit-printr-un-scam
32.DNSC, Ați fost victima unui furt al datelor de card sau de date bancare? Disponibil pentru download direct, la: https://dnsc.ro/vezi/document/ce-fac-daca-mi-s-au-furat-datele-de-card-sau-de-date-bancare
33.DNSC, Campanie de prevenire a criminalității informatice în rândul tinerilor. Disponibil la: https://dnsc.ro/pagini/campania-prevenire-criminalitate-informatica
34.DNSC, Contul dumneavoastră de pe o platformă de comunicare socială a fost atacat de hackeri? Disponibil pentru download direct, la:
https://dnsc.ro/vezi/document/ce-fac-daca-mi-a-fost-compromis-un-cont-online
35.DNSC, Our contact information. Disponibil la:
https://dnsc.ro/contact
36.DNSC, Pagina web oficială. Disponibil la:
https://dnsc.ro/
37.ECDL Foundation 2014, Eroarea "Nativ Digital". Disponibil pentru download direct, la:
https://www.ecdl.ro/uploads/stiri/resources/files/E%C5%9Fecul_Genera%C5%A3iei_Nativilor_Digitali_Document_de_pozitie.pdf
38.EDPB, Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, Versiunea 1.1, Adoptate la 4 mai 2020. Disponibil pentru download direct, la:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_ro.pdf
39.ESET, Digital Security Handbook For Teachers. Disponibil pentru download direct, la:
https://saferkidsonline.eset.com/storage/free-downloads/October2021/ISyOqDcONESXDjvx61fW.pdf
40.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
41.ESET, Parental control. Disponibil după crearea unui cont personal, aici:
https://parentalcontrol.eset.com/
42.European Commission, What is personal data? Disponibil la:
https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en
43.Google AI, Making AI helpful for everyone. Disponibil la:
https://atozofai.withgoogle.com/intl/en-US/
44.Google Family Link, Help keep your family safer online. Disponibil la:
https://families.google.com/familylink/
45.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
46.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/
47.Internet Matters, Because children deserve a safe digital world. Disponibil la:
https://www.internetmatters.org/
48.Legea nr. 272/2004 privind protecția și promovarea drepturilor copilului. Disponibil la:
https://legislatie.just.ro/Public/DetaliiDocument/156097

49.Matthew Sparkes, What does Wi-Fi stand for? Disponibil la:
https://www.newscientist.com/question/what-does-wi-fi-stand-for/
50.Medicover, Ciuma – o boala infecțioasă care încă nu a fost eradicată. Disponibil la:
https://www.medicover.ro/despre-sanatate/ciuma-o-boala-infectioasa-care-inca-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.RON&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=IwAR1UCwlo8DlaHfgzTDtyklb2AIWdtvNpVB2PYrvrFQi6zj8ieRUERSRmuzo
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 „uitate" ale acestora. Disponibil la:
https://www.avocatnet.ro/articol_44911/Libertatea-de-exprimare-a-copiilor-este-doar-unul-dintre-drepturile-%E2%80%9Euitate-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%AEn%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-HnpsrJifRsYoeFq