SECURITATEA INFORMATICĂ ȘI SIGURANȚA COPIILOR ÎN MEDIUL ONLINE

Petru-Dan Kovaci
Security Engineer,
IT Security & Coding Trainer IT Level

ITLEVEL
DEPĂȘEȘTE-ȚI NIVELUL!

CINE SUNTEM NOI?

- ITLevel este centrul de excelență în Programare, Robotică, Dezvoltare de jocuri, IT și Matematică, născut din pasiunea pentru înalta tehnologie și din dorința de a le insufla copiilor încrederea în viitorul lor digital.
- De la înființare, dîn anul 2018 și până astăzi, ITLevel a devenit centrul educațional cu cea mai bogată ofertă de cursuri pentru copii cu vârste cuprinse între 8 și 18 ani, dar și pentru adulți.

  Sub sloganul ”Depășește-ți nivelul”, ITLevel livrează peste 25 de cursuri interactive, la cele mai înalte standarde profesionale, adaptate cerințelor industriei IT, ce oferă pregătirea necesară pentru viitoarea carieră de succes a copiilor și a adulților.
- Pasiunea și dorința de a fi cel mai bun te ajută să îți împlinești visurile!
- Prin dezvoltarea continuă din acești ani, ITLevel a reuşit să atragă în echipa sa olimpici internaționali și naționali, multiplu medaliați, doctori în informatică, experți cu cele mai înalte certificări, cu o solidă expertiză tehnică.
- ITLevel are ca misiune dezvoltarea personală a cursanților, dobândirea cunoștințelor în diferite tehnologii și cultivarea spiritului competitiv şi de echipă prin organizarea de concursuri cu premii, recunoscute de Ministerul Educației, care răsplătesc ideile creative, inovația, munca și perseverența, dar și prin organizarea de workshop-uri și evenimente la care cursanții participă gratuit.
- Cursurile se desfașoară atât online cât și în săli de instruire ultramoderne dotate cu display interactiv, tablete grafice, laptopuri, roboți educaționali și senzori de pe stația spațială internațională, pentru a oferi un mediu propice dobândirii cunoștințelor în domeniul IT, la cele mai înalte standarde.
- Lucrăm cu grupe mici de 4 - 8 cursanți.
- Suntem parteneri strategici pentru școli și universități, dar nu numai.
- La ITLevel punem accent pe performanță!

INTRODUCERE

- Este important să discutăm despre siguranța copiilor în mediul online, deoarece generația actuală petrece o cantitate semnificativă de timp folosind computere, tablete, smartphone-uri și alte dispozitive conectate la internet.
- Această conectivitate sporită prezintă multe beneficii, dar îi și expune pe copii la noi provocări și pericole.
- Voi prezenta **riscurile** la care sunt expuși cei mici și care sunt **metodele** pe care le pot utiliza pentru a se proteja, iar apoi voi oferi câteva **sfaturi** pentru părinți și profesori, pentru a-i ajuta pe copii să evite expunerea periculoasă la mediul online.

Secțiunea 1 – Să înțelegem riscurile

Conținut dăunător

Cu nenumărate resurse disponibile online, este ușor pentru copii să dea peste materiale explicite, limbaj sugestiv sexual sau scene violente. Accesul la aceste resurse le poate influența negativ atitudinile față de lumea din jur și pot adopta comportamente nepotrivite.

Dezinformare

Copiii se bazează frecvent pe informațiile găsite cu ajutorul motoarele de căutare, fluxurile de știri sau postările pe rețelele sociale. Din păcate, faptele neverificate, farsele, teoriile conspirației sau propaganda vehiculată online pot modela **credințe greșite sau concluzii false**, împiedicând **gândirea critică** și rezolvarea problemelor.

Dependență și probleme de sănătate

Petrecerea excesivă a timpului pe dispozitivele digitale poate contribui la probleme precum activitatea fizică insuficientă, alimentația deficitară, privarea de somn, problemele de vedere sau chiar afecțiuni mentale precum ADHD sau depresia. Aceste complicații se pot transmite până la vârsta adultă și pot afecta negativ starea de bine pe termen lung.

Furt de identitate

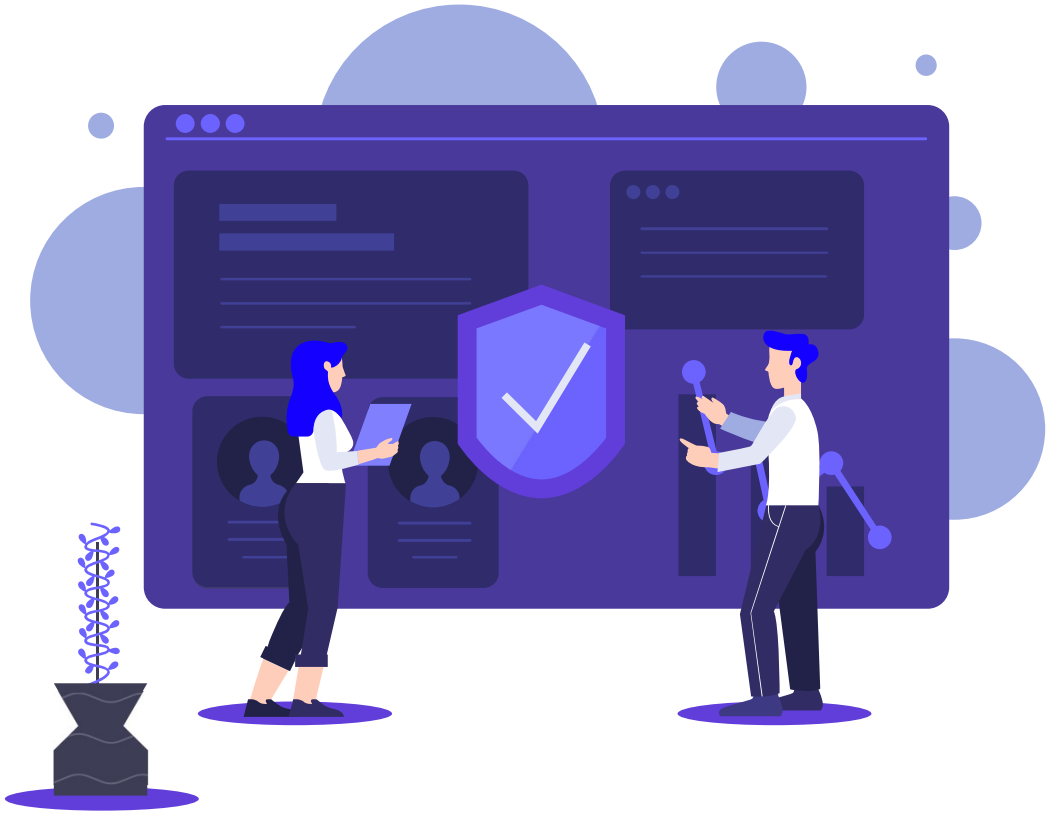
Copiii sunt în mod special predispuși să divulge **informații confidențiale** (de exemplu, **nume complete, adrese, parole**) în timp ce vorbesc cu prietenii sau joacă jocuri online. Această dezvăluire ar putea duce la furt de identitate, escrocherii financiare sau, mai rău, un potențial pericol pentru viața lor

CYBERBULLYING - riscuri

Pe măsură ce copiii petrec mai mult timp interacționând cu alte persoane prin intermediul aplicațiilor de mesagerie, al rețelelor sociale și al comunităților de jocuri, ei devin susceptibili victimizării online.

CYBERBULLYING

Efecte



Izolare socială

Victimele cyberbullying-ului s-ar putea retrage din cercurile sociale, ar putea evita să meargă la școală sau la evenimente/activități de grup.

Frică/ anxietate/ depresie

Expunerea pe termen lung la cyberbullying poate contribui la simptome de depresie, cum ar fi tristețea, lipsa de speranță sau pierderea interesului pentru activitățile de care s-au bucurat odată.

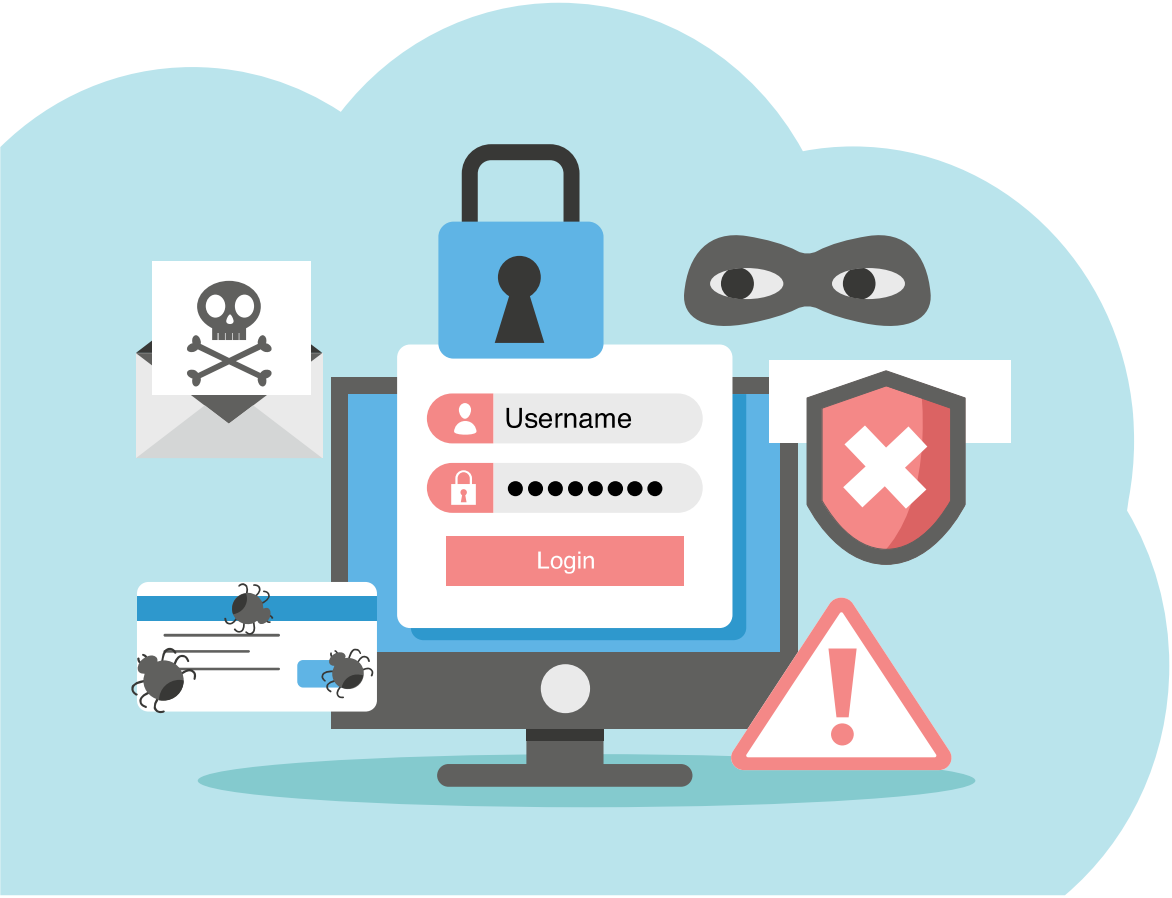
Rezultate academice slabe

Experiențele de cyberbullying pot distrage atenția copiilor de la concentrarea asupra studiilor, ceea ce duce la note mai scăzute sau la dezinteresul total pentru educație.

Consumul de substanțe interzise

Acest viciu se poate dezvolta ca o modalitate de a face față sentimentelor copleșitoare asociate cu hărțuirea cibernetică.

Tipuri de *atacuri cibernetice* cu care copiii se pot confrunta



PHISHING

Atacatorii trimit **mesaje frauduloase** pretinzând a fi surse legitime pentru a păcăli victimele să ofere informații confidențiale sau să facă click pe linkuri rău-intenționate. Copiii ar trebui să învețe să identifice *red flags*, cum ar fi **adrese URL suspecte** și **e-mailuri necunoscute** care solicită date personale.

MALWARE

Programul malware reprezintă **orice software conceput intenționat** pentru a provoca daune, a fura date sau a interfera cu operațiunile normale ale computerului. Copiii trebuie să evite descărcarea de atașamente suspecte sau vizitarea site-urilor web dubioase care ar putea infecta dispozitivele cu viruși sau ransomware.

RANSOMWARE

Acest tip de atac **criptează fișierele de pe computerul victimei** până când se efectuează plata pentru restabilirea accesului. Învățarea copiilor să facă în mod regulat copii de rezervă pentru documentele esențiale poate atenua daunele cauzate de ransomware.

Metode de protecție a datelor

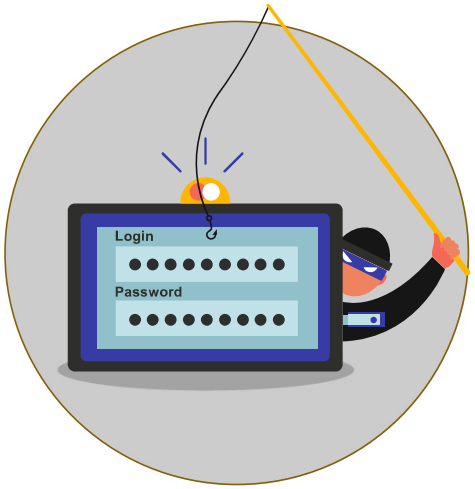
Pașii pe care copiii îi pot urma pentru a-și proteja confidențialitatea în timp ce folosesc platforme online

Social Media

Selectarea publicului pentru postări, restricționarea opțiunilor de etichetare, dezactivarea partajării locației și examinarea solicitărilor de prietenie.

→

Aceste măsuri ajută la reglementarea celor ce au acces la informațiile personale și reduc șansele de a intra în legătură cu străinii.



Logare

Utilizarea de aliasuri sau porecle pentru conturile de e-mail și configurarea de parole puternice. Activarea autentificării în doi pași pentru un plus de securitate.

→

Crearea unui pseudonim și consolidarea protecției autentificate ajută la siguranța informațiilor personale.

Conținut foto/video

Ștergerea în mod regulat a videoclipurile vechi care conțin informații personale sau conținut sensibil și implementarea setărilor de confidențialitate.

→

Gestionarea conținutului existent și implementarea setărilor de confidențialitate reduce probabilitatea expunerii datelor personale.

Metode de protecție a datelor

Pașii pe care copiii îi pot urma pentru a-și proteja confidențialitatea în timp ce folosesc platforme online

Aplicații de chat

Setarea unor limitări de vizibilitate a chat-ului între persoane de contact sau grupuri, refuzarea solicitărilor de prietenie aleatorii de la străini. Copilul să fie precaut atunci când distribuie povești personale sau imagini care nu sunt destinate unui public larg și să ia în considerare utilizarea instrumentelor de comunicare criptate *end-to-end* pentru o asigurare sporită a confidențialității.

→

Implementarea filtrării contactelor și expunerea cu prudență în ceea ce privește conținutul partajat protejează informațiile personale. Utilizarea aplicațiilor criptate poate adăuga un strat suplimentar de protecție.

Tips pentru părinți/ profesori

01

CONFIGURAREA CONTROLULUI PARENTAL

Majoritatea dispozitivelor și furnizorilor de servicii de internet oferă funcții de control parental încorporate care permit **restricționarea accesului la anumite site-uri sau tipuri de conținut** pe baza vârstei.

02

TIMPUL PETRECUT ÎN FAȚA ECRANULUI

Stabilirea unor reguli clare cu privire la cât timp pot petrece copiii pe computer, tabletă sau smartphone în fiecare zi, precum și restricții privind orele din zi în care pot folosi aceste dispozitive, dar și **conținutul** pe care îl accesează online.

03

PRACTICI SIGURE PE INTERNET

Educarea copiilor despre **comportamentul online adecvat** și despre importanța protejării informațiilor personale. Discutați subiecte precum hărțuirea cibernetică, prădătorii online și potențialele pericole de a partaja prea multe informații online.

04

MONITORIZAREA ACTIVITĂȚII ONLINE

Verificați în mod regulat **istoricul** browserului copilului dvs., interogările de căutare, postările pe rețelele sociale și orice fișiere descărcate pentru a fi informat despre obiceiurile sale online și pentru a detecta potențialele *red flags* din timp.

05

RESTRICȚIONAREA ANUMITOR APLICAȚII

Dacă există anumite programe sau aplicații care vă îngrijorează datorită naturii sau popularității lor în rândul celor mici, luați în considerare **blocarea accesului direct** la acestea. Acestea ar putea include aplicații de rețele sociale, servicii de chat sau platforme de jocuri online.

CONCLUZIE

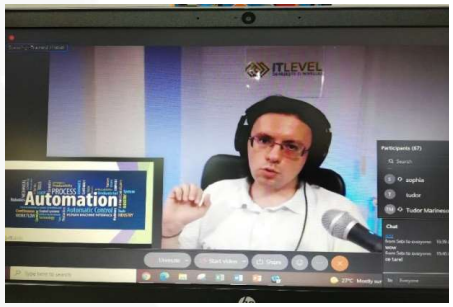
Protejarea copiilor în mediul online necesită implicarea părinților, eforturi educaționale, colaborare între liderii industriei, factorii de decizie politică și societatea în ansamblu.

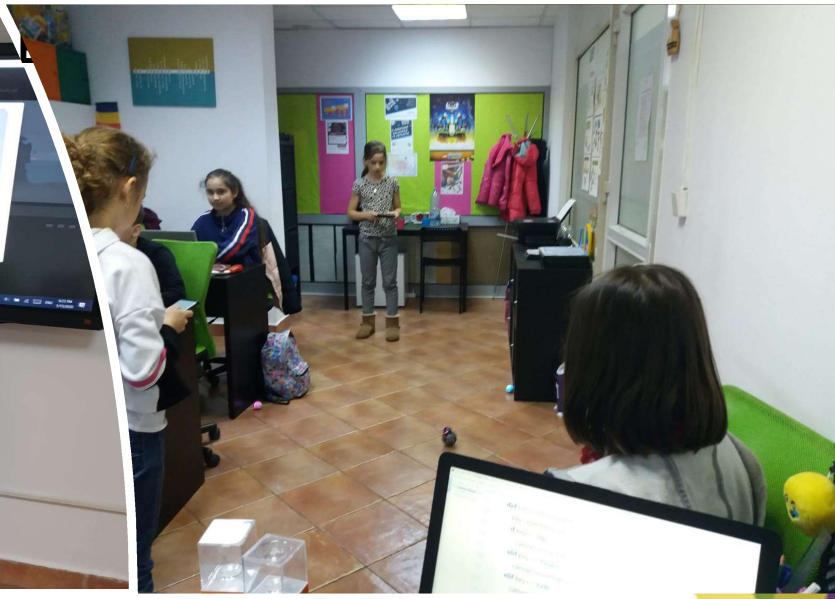
Luând **măsuri proactive**, cum ar fi crearea de motoare de căutare și rețele sociale adaptate copiilor, aplicarea restricțiilor stricte de vârstă, oferirea de controale solide de confidențialitate, monitorizarea conținutului generat de inteligența artificială, furnizarea de linii directoare extinse de siguranță, putem deschide calea către o experiență online mai incluzivă, transparentă și echitabilă pentru generațiile viitoare.

Este responsabilitatea noastră colectivă să ne asigurăm că internetul continuă să evolueze într-un spațiu care încurajează creativitatea, învățarea, inovația și creșterea, acordând în același timp **prioritate siguranței, bunăstării și confidențialității pentru toți.**

ITLEVEL
DEPĂȘEȘTE-ȚI NIVELUL!

Cum experimentăm la ITLevel?





#campioniisuntaici

www.itlevel.ro

0751.011.391


ITLEVEL
DEPĂȘEȘTE-ȚI NIVELUL!
Vă mulțumesc
și
vă aștept la cursurile ITLevel
pentru securitatea dvs și pentru
un spațiu cibernetic mai sigur pentru noi toți!
www.itlevel.ro
0751.011.391