certSIGN

Cyber4Kids

Manual de educaţie cibernetică pentru copii şi părinţi

cyber4kids.ro

certSIGN

Cyber4Kids

CUPRINS

certSIGN

Cyber4Kids

LECŢIA 1.
Jocurile mobile, în siguranţă

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – INELUL VICTORIEI! Aşa te vei putea juca în siguranţă pe telefonul mobil sau pe tabletă!

1. **JOC NOU.** Cel mai bine instalezi împreună cu părinţii jocurile noi. Ei îţi vor spune dacă sunt potrivite pentru tine, astfel încât să te poţi juca în siguranţă!

2. **CUM TE CHEAMĂ?** Atunci când îţi alegi un nume pentru joc, nu folosi în el numele tău adevărat, vârsta sau data naşterii.

3. **PE CHAT.** Unele jocuri au chat-uri în care poţi scrie mesaje sau vorbi live cu ceilalţi jucători. Nu uita să te porţi frumos cu fiecare! Dacă cineva nu vorbeşte frumos cu tine, părăseşte discuţia.

4. **DATE SECRETE.** Dacă un alt jucător îţi cere să îi spui numele tău, unde locuieşti, la ce şcoală înveţi sau îţi cere să vă vedeţi într-un loc anume, să nu îi răspunzi! Aceste date sunt secrete!

5. **LINK-URI.** Tot pe chat este posibil să primeşti link-uri de la alţi jucători - nu le deschide! Mesajele pot fi trimise de răufăcători sub acoperire iar acele link-uri pot fi capcane!

6. **DESPRE BANI.** Când te joci, sigur vei vedea mesaje care îţi oferă, în schimbul unor bani, mega-puteri sau o armă nouă pentru personajul tău! Unele îţi pot promite să te scape de reclamele care îţi întrerup aventura. Refuză şi închide aceste mesaje care îţi cer să plăteşti.

PAGINA PĂRINȚILOR

Verifică întotdeauna aplicaţiile/jocurile, preferabil înainte de descărcare şi utilizare:
• fereşte-te de jocuri listate în terţe platforme (în afară de Google Play / App Store - nu este exclusă existenţa unor aplicaţii cu malware nici aici, dar riscul este mult mai redus);
• consultă întotdeauna recenziile – cele din mai mult de două cuvinte şi cu un limbaj natural;
• caută informaţii online despre dezvoltatorul jocului pentru a verifica legitimitatea acestuia;
• utilizează o soluţie antivirus pentru securitate mobilă.

Configurează controlul parental pe Google Play/App Store pentru:
• blocarea aplicaţiilor pe care nu vrei să le folosească copilul;
• blocarea descărcărilor sau achiziţiilor, în funcţie de nivelul de maturitate al conţinutului;
• blocarea automată a ecranului dispozitivului mobil utilizat de copil, pentru ora de culcare.

Consultă întotdeauna evaluarea conţinutului (eticheta PEGI - Pan European Game Information) şi recenziile unui joc, pentru a te asigura că este adecvat vârstei copilului.

Evită achiziţiile accidentale sau nedorite folosind protecţia prin autentificare (solicitare parolă/ PIN înainte de efectuarea oricărei achiziţii). Păstrează aceste date doar pentru tine.

Proba practică – alocă-ţi câteva minute pentru a "testa" personal jocul. Veţi avea un nou subiect de discuţie comun, veţi petrece timp împreună iar copilul se va bucura de interacțiunea cu tine.

Discută frecvent despre experienţa avut de copil în joc, încurajându-l să-ţi spună dacă cineva îl agresează verbal, îi cere date personale, imagini nepotrivite sau îl face să se simtă inconfortabil.

Ia în calcul dezactivarea camerei web / microfonului în cazul jocurilor unde este posibil acest lucru.

Descoperă mai multe pe cyber4kids.ro!

certSIGN

certSIGN

Cyber4Kids

LECŢIA 2.
Datele personale sunt secrete

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic - PELERINA INVIZIBILITĂŢII! Aşa vei putea ascunde în siguranţă datele personale secrete!

1 **CE DATE PERSONALE SUNT SECRETE?** Nu oferi niciodată şi nici nu posta TU public pe Internet:

- numele tău complet, data naşterii, vârsta;
- adresa de acasă sau şcoala la care înveţi;
- numărul de telefon şi adresa de e-mail;
- datele de pe cardurile bancare ale părinţilor;
- orice alte informaţii despre tine sau familia ta.

2 **2. CUM?** Răufăcătorul de pe Internet îţi poate cere datele personale secrete prin mesaje trimise pe Facebook, YouTube, Instagram, WhatsApp sau TikTok, în jocurile online pe care le joci pe telefon, tabletă sau calculator, prin chat sau discuţii live, printr-un e-mail sau într-un formular online.

3 **CINE?** Răufăcătorul poate fi un adult rău intenţionat care se preface că este prietenul tău online - de aceeaşi vârstă cu tine, o persoană importantă, o rudă sau o cunoştinţă, pentru a te convinge să îi spui date personale secrete. Sau te poate minţi că vei primi ceva super interesant (un telefon, un joc nou) în schimbul unor informaţii despre tine sau familia ta.

4 **ŞŞŞŞT, SECRET!** Dacă răufăcătorii obţin datele personale secrete, vor putea – de exemplu – să te urmărească acasă sau la şcoală şi să îţi facă rău. Sau să creeze conturi false pe Internet şi să pretindă că eşti tu!

PAGINA PĂRINȚILOR

1. CE DATE PERSONALE? Realizaţi împreună o listă cu informaţiile care nu trebuie divulgate pe Internet de copil – nici atunci când i se cer, dar nici din proprie iniţiativă, în conversaţii sau postări publice. Regula secretului se aplică nu doar pentru datele sale personale, ci şi pentru cele ale prietenilor şi colegilor! Acolo unde este posibil (jocuri online, platforme social media, quizz-uri etc.) completează strict câmpurile obligatorii, utilizează un pseudonim, oferă cât mai puţine informaţii.

2. LA CINE AJUNG DATELE PERSONALE? Copilului i se poate părea normal să împărtăşească prietenilor virtuali tot felul de informaţii. Doar sunt prieteni, nu? Explică-i faptul că, pe Internet, nu toată lumea este cine susţine, mai ales dacă vorbim despre persoane cu care a avut contact exclusiv on-line.
Chiar dacă cineva arată în poze, scrie sau se comportă ca un copil, cei mici pot fi păcăliţi. Cel mai sigur este să înţeleagă că trebuie să fie întotdeauna precaut(ă) și să nu dea niciodată informații personale.

3. PRIETENI PE SOCIAL MEDIA. În cazul anumitor platforme de social media unde este posibil acest lucru, precum Facebook, Instagram sau TikTok, este bine să fii în lista de prieteni / urmăritori ai copilului.
Astfel vei putea monitoriza postările text, fotografiile, clipurile video încărcate, respectiv comentariile la acestea şi reacţiona în timp util dacă includ date personale.
Tot pe social media, alege setările de confidenţialitate optime pentru contul copilului - privat, nu public. Limitează publicul care poate vedea conţinutul postat şi informaţiile personale (cu cât mai puţine, cu atât mai bine) doar la lista de prieteni.

4. DIN GREŞELI SE ÎNVAŢĂ. Stai liniștit(ă) dacă copilul tău greșește, postând ceva ce nu ar trebui. Ajută-l să șteargă postarea și discutați împreună despre cum poate evita o greșeală similară în viitor. Dacă reacţionezi exagerat sau îi refuzi accesul, este posibil să nu mai apeleze la tine pentru ajutor.

5. PUTEREA EXEMPLULUI. Ştim că eşti mândru/mândră de copilul tău, însă rezistă tentaţiei de a posta în social media, grupuri sau forumuri on-line informaţii, poze sau filme. De exemplu, nu posta fotografii sau clipuri video din prima zi de şcoală, cu adăugarea locaţiei, sau de la aniversarea copilului, în ziua evenimentului, eventual cu menţionarea vârstei (sau cifra de pe tort). Deşi datele personale nu sunt oferite explicit, ele pot fi cu uşurinţă deduse. Tu eşti primul şi cel mai bun exemplu pentru copilul tău!

certSIGN

Cyber4Kids

LECŢIA 3.

Cine te păcăleşte on-line? Identităţi false

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – OCHELARII ADEVĂRULUI! Aşa vei putea recunoaşte minciunile răufăcătorilor care pretind că sunt altcineva pe Internet!

1 **PRIETENI ON-LINE?** Atenţie la persoanele care îţi cer prietenie sau încep să vorbească cu tine prin mesaje on-line pe Facebook, YouTube, Instagram, WhatsApp, TikTok sau în chat-urile din jocuri. Pot fi infractori care mint despre cine sunt şi vârsta lor, pentru a-ţi face rău!

2 **DE CE?** Răufăcătorii de pe Internet care mint despre cine sunt:

• vor să râdă de tine şi să facă glume pe seama ta – ei fură identitatea unei persoane reale sau inventează una. Pot fi chiar copii care te cunosc în realitate şi care pretind că sunt altcineva.

• vor să obţină datele tale personale şi informaţii despre familia ta;

• vor să obţină poze şi filmuleţe cu tine sau vor să vă întâlniţi în realitate.

3 **CUM TE FEREŞTI?** Respectă de fiecare dată aceste sfaturi:

• nu accepta cererile de prietenie şi nu răspunde la mesajele şi comentariile necunoscuţilor;

• nu oferi on-line date personale, poze, filmuleţe şi orice alte informaţii despre tine sau familia ta;

• nu crede pe cuvânt tot ce spun cei care te contactează pe Internet;

• nu răspunde la provocările făcute de prietenii virtuali, dacă par nepotrivite şi nu te-ar face să te simţi în siguranţă;

• spune-le părinţilor despre persoanele care vorbesc cu tine on-line, mai ales dacă îţi spun, trimit sau cer lucruri care te fac să te simţi ciudat;

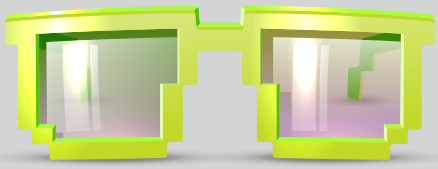
• nu pretinde TU pe Internet că eşti altcineva, doar pentru a face o glumă.

PAGINA PĂRINŢILOR

1. DISCUTAŢI DESPRE IDENTITĂŢI FALSE. Explicaţi-i copilului că, pe Internet, există multe persoane care mint despre cine sunt cu adevărat (inclusiv despre vârsta lor), de cele mai multe ori având scopuri rău intenţionate.
Cel mai sigur este să nu accepte cererile de prietenie şi să nu răspundă la mesajele necunoscuţilor care solicită date personale sau imagini şi clipuri video cu el/ea decât DUPĂ ce s-au consultat cu tine sau un cu un alt adult de încredere (rudă, cadru didactic etc.).

2. ECHIPA DETECTIVILOR! Realizaţi împreună "exerciţii" de recunoaştere a conturilor false:
• fotografia de profil – lipsa acesteia, o imagine generalistă sau neclară, existenţa unei singure fotografii-portret cu fizionomia respectivă sunt semnale de alarmă;
• vechimea şi conţinutul profilului – un cont realizat în urmă cu puţin timp, cu foarte puţine postări şi interacţiuni, informaţii biografice lipsa, minimale sau care nu se regăsesc în alte search-uri on-line, poate fi fals;
• preteni comuni – existenţa unui cerc de prieteni comuni este esenţială. Chiar şi aşa, prietenul unui prieten on-line rămâne un străin;
• verificare în realitate – în cazul cererilor de prietenie primite de la persoane care susţin că au auzit de copil de la altcineva / sunt cunoştinţe ale unei terţe persoane, de verificat cu aceasta din urmă realitatea informaţiilor.

3. MESAJE PERICULOASE. Oferă-i copilului exemple concrete de mesaje periculoase la care nu trebuie să răspundă, precum:



• *"Bună, postările tale sunt super, îmi dai numărul tău de telefon să vorbim pe WhatsApp?"*
• *"Hei, sunt fratele colegei tale de clasă / prietenei tale (+ nume din lista de prieteni). Îmi poţi da adresa ta? Am ceva să îţi dau de la ea."*
• *"Pozele / filmuleţele tale sunt grozave! Dă-mi şi mie follow să vorbim mai multe!"*
• *"Hey, îţi place poza asta cu mine? Dă-mi şi mie una cu tine."*.

4. MĂSURI DE PRECAUŢIE. Întotdeauna creaţi împreună conturile pe platformele de social media, preferabil fii primul prieten din lista copilului şi monitorizează pe cât posibil postările şi conversaţiile din acestea, dar şi din chat-urile din jocuri.
Setează conturile ca private, limitând publicul care poate transmite cereri de prietenie, mesaje directe, distribui sau comenta, doar la lista de prieteni (sau nimeni).
Blocaţi împreună utilizatorii cu interacţiuni nepotrivite şi mesajele de la aceştia.
Încurajează utilizarea dispozitivelor mobile şi a laptopului / calculatorului doar pentru anumite perioade de timp, într-o cameră comună în care se află şi un adult.

certSIGN

Cyber4Kids

LECŢIA 4.
Linkuri periculoase

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – BRĂŢARA REALITĂŢII! Ea te va ajuta să recunoşti linkurile false, în spatele cărora se ascund viruşi şi infractori cibernetici!

1 **VIRUŞI ŞI PROGRAME PERICULOASE.** Răufăcătorii de pe Internet îţi pot trimite linkuri în spatele cărora se ascund viruşi, programe şi mesaje periculoase, care îţi vor strica telefonul, tableta sau calculatorul ori îți vor fura datele personale, fără să îţi dai seama.

2 **CLICK AICI!** Ca să fie siguri că dai click, infractorii vor minţi şi vor spune că la acel link poţi vedea sau descărca un filmuleţ / un joc super amuzant. Sau îţi pot promite că, dacă intri pe acel site şi le dai date personale, vei câştiga mulţi bani, un telefon, o tabletă, o jucărie, noi puteri în jocul tău preferat on-line.

3 **CUM TE FEREŞTI?** Respectă de fiecare dată aceste sfaturi:

- **nu da click pe orice link** de pe Internet sau pe care îl primeşti, mai ales dacă este de la o persoană necunoscută;
- **nu crede** mesajele care îţi promit că vei primi ceva valoros – pe Internet nimic nu este gratis;
- **nu descărca** jocuri, muzică, filme sau orice altceva din site-uri sau din e-mailuri trimise de persoane necunoscute;
- **verifică** dacă linkurile pe care ai intrat au în faţa adresei un lacăt închis – acest lucru înseamnă că sunt sigure pentru tine;
- **nu oferi date personale sau parole** în site-urile de pe Internet, în chestionare, ca răspuns la e-mailuri sau mesaje pe telefon;
- **întreabă-i mai întâi pe părinţi** dacă ar fi bine să deschizi un link sau un site.

PAGINA PĂRINŢILOR

1. RISCURI. Explică-i copilului care sunt riscurile la care este expus – simpla accesare a unui link / site web sau descărcare a unui ataşament poate duce la instalarea automată de programe malware pe dispozitiv. Acestea pot oferi acces altor persoane la telefon, tabletă sau calculator.

2. PROBA PRACTICĂ. Învaţă-l cum să verifice autenticitatea link-urilor, site-urilor şi a e-mailurilor primite:

• **LINK.** Nu începe cu https:// ci cu http://? Lipseşte din faţa URL-ului (în partea stângă) un lacăt mic? **Nu este sigur.**

• **SITE.** URL-ul nu corespunde cu informaţia afişată în pagină (de exemplu, în adresa site-ului literele sunt înlocuite de cifre sau cuvintele sunt scrise greşit – c0npanle)? Lipseşte din pagină logo-ul? Sunt multe greşeli de scriere în textul afişat sau acesta este scris foarte mic? Apar multe pop-up-uri? Te anunţă că ai câştigat ceva? Solicită informaţii personale? **Nu este sigur.**

• **E-MAIL.** Nu recunoşti persoana / sursa care ţi-a transmis mesajul? Ţi se oferă ceva gratuit sau te anunţă că ai câştigat ceva? Mesajul ţi-a fost transmis on-line de un prieten dar când ai verificat cu acesta în realitate (obligatoriu) nu s-a verificat? Solicită informaţii personale sau parole? Sunt multe greşeli de scriere în textul afişat sau acesta este scris foarte mic? **Nu este sigur.**

3. SOLUŢII ANTIVIRUS. Curiozitatea este naturală pentru cei mici, ei fiind mereu atraşi de lucruri noi şi putând accesa cu ușurință linkuri maliţioase sau descărca jocuri din locații web necunoscute. De aceea, instalarea unei soluții antivirus, care include un motor de scanare în timp real, firewall și actualizare automată, este esenţială. O astfel de soluţie te ajută împotriva unor probleme precum spyware și viruși de pe site-urile pe care copilul le accesează.

Linkuri / site-uri aparent legitime pot conține coduri malware sau pot redirecționa către un site fals care arată la fel, dar care conține de fapt un keylogger (program care înregistrează fiecare bătaie de tastă şi salvează aceste date într-un fişier) sau un virus.

Efectuează periodic verificări automate de viruși şi scanări profunde ale sistemului, pentru a te asigura că nu există “vizitatori” nedoriţi şi că informațiile personale ale copilului nu sunt colectate.

4. SOLUŢII DE CONTROL PARENTAL. Cu ajutorul unei soluţii de control parental (atât pentru dispozitivele mobile, cât şi pentru cele desktop) puteţi monitoriza experiența pe Internet a copilului - de la timpul permis să-l petreacă on-line, până la aplicațiile și site-urile web utilizate / accesate. Încercările de utilizare a programelor blocate vor fi oprite și înregistrate în jurnalul programului, pentru vizualizare ulterioară.

certSIGN

Cyber4Kids

LECŢIA 5.
Internetul nu uită!

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – JURNALUL AVENTURII! În el vei putea strânge amintiri de neuitat şi te va ajuta să le arăţi celorlalţi lucrurile grozave despre tine!

1. **INTERNETUL NU UITĂ!** Chiar dacă schimbi sau ştergi ce publici on-line (postări, comentarii, poze şi filmuleţe, mesaje), vor fi persoane care au văzut deja ce ai publicat. Poate chiar au descărcat, transmis la altcineva sau au făcut o captură de ecran (o poză) cu ce ai postat. Atunci când ştergi informaţii de pe Internet nu înseamnă că ele dispar pentru totdeauna!

2. **DISTRACTIV!?** Postările care ţi se par acum în regulă s-ar putea să nu ţi se mai pară la fel de distractive atunci când vei creşte. Nici ţie şi nici altora – pentru că oricine va putea să găsească orice ai postat, acum 10 sau chiar 20 de ani, să te judece sau să râdă de tine! Cei care nu te cunosc vor putea să afle o grămadă de informaţii despre tine on-line şi să îşi facă o părere greşită!

3. **AŞ FACE ASTA ŞI ÎN REALITATE?** De fiecare dată când vrei să postezi, gândeşte-te dacă:

• ai face aceeaşi glumă, ai folosi aceleaşi cuvinte şi ai spune aceleaşi lucruri despre o persoană şi dacă ai fi faţă în faţă cu ea?
• pozele şi filmuleţele postate pe Internet cu tine li s-ar părea distractive şi părinţilor tăi? Ce faci în ele este corect şi politicos?
• ai spune unui străin pe care îl întâlneşti pe stradă numele tău, unde locuieşti, informaţii despre familia ta, ai accepta cadouri şi ai merge cu el oriunde?

Dacă răspunsul este nu, atunci **NU** face toate aceste lucruri doar pentru că eşti în spatele unui telefon, al unei tablete sau unui calculator.

PAGINA PĂRINȚILOR

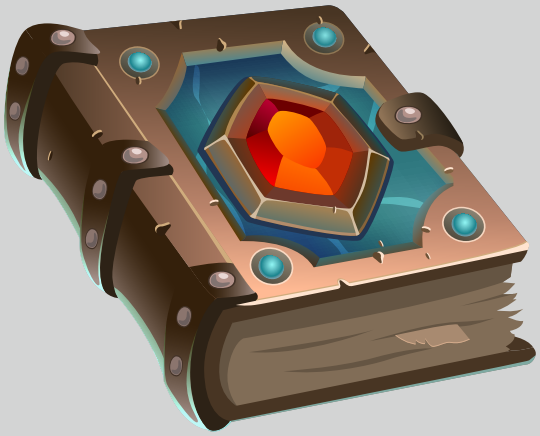
1. CE POSTEZI ON-LINE (AMPRENTA DIGITALĂ) CONTEAZĂ! Explică-i copilului importanţa amprentei digitale – fiecărei acţiuni realizate pe Internet îi este asociată o înregistrare digitală, aceasta fiind stocată on-line pentru a fi accesată în orice moment – de noi şi, cel mai important, de oricine altcineva.

De la postări text şi fişiere media nu tocmai fericite pe reţelele de socializare, la date personale publicate şi indexate on-line – fiecare informaţie contribuie la modul în care suntem percepuţi, cu potenţiale repercusiuni negative pe termen mediu şi lung.

De exemplu, multiple facultăţi şi companii realizează căutări pe Internet înainte de a accepta candidaţi iar informaţii despre noi poate să afle orice străin, mai mult sau mai puţin bine intenţionat. Menţinerea unei reputații pozitive atât online, cât și offline, este esenţială!

2. DE CE NU UITĂ INTERNETUL? Realizaţi împreună un mic test, astfel încât copilul să înţeleagă puterea Internetului de a reţine – tastează numele tău sau al unei persoane cunoscute într-un motor de căutare şi apoi navigaţi împreună prin rezultatele afişate.

Veţi observa că sunt acoperite o gamă variată de informaţii – de la postări, la imagini, clipuri video, până la comentarii şi orice alte activităţi pe site-uri.



Însă, cel mai important este să înţelegeţi că eliminarea acestui conţinut digital poate fi de la foartea simplă (cu un simplu click pe opţiunea de “Ștergere”), la foartea dificilă (solicitarea motoarelor de căutare sau a proprietarilor de site-uri web să o elimine), până la imposibilă – nu avem aproape niciun control asupra modului în care comunitatea on-line ne utilizează datele şi conţinutul publicat (cine le descarcă, le copiază sau le pune la dispoziție în altă parte).

3. CHIAR ESTE DISTRACTIV? Nu puţine sunt situaţiile în care postarea anumitor fotografii, clipuri video ori comentarii au avut efecte negative pentru “titularii” acestora. Impulsurile de moment şi opiniile din trecut se pot întoarce peste câţiva ani împotriva noastră.

Câteva exemple edificatoare în acest sens, ce pot fi date copilului, pentru a înţelege mai bine riscurile la care se expune atunci când postează orice, fără aplicarea unui “filtru”:

- imagini sau filme publicate pe canale de socializare în diverse ipostaze care nu îl avantajează, inacceptabile social sau scoase din context (devenite virale, transformate în meme-uri, prelucrate digital);
- postări injurioase sau cu un limbaj vulgar.

certSIGN

Cyber4Kids

LECŢIA 6.
Cyberbullying

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – TALISMANUL PRIETENIEI! Acesta te va proteja în faţa celor care nu se poartă frumos cu tine on-line!

1 **CE ÎNSEAMNĂ CYBERBULLYING?** Atunci când cineva se poartă urât cu tine pe Internet, devenind un agresor – o persoană care vrea să te necăjească şi să râdă de tine. De exemplu, îţi scrie mesaje supărătoare sau te ameninţă, spune minciuni despre tine ori îţi dă porecle răutăcioase, ba chiar îndeamnă alte persoane să se poarte urât cu tine. Sau încearcă să îi păcălească pe alţii on-line, pretinzând că eşti tu şi postând informaţii, fotografii sau filmuleţe jignitoare, fără să ştii sau să fii de acord.

2 **CUM TE PROTEJEZI?** Urmează de fiecare dată aceste sfaturi:

- **vorbeşte cu un un prieten dar, mai ales, cu un adult de încredere** - părinţii tăi, o rudă, profesorii te pot ajuta;
- **nu răspunde la mesajele, comentariile sau postările agresorilor** - dacă cineva te-a supărat este posibil să spui lucruri pe care le vei regreta mai târziu;
- **blochează şi raportează agresorii** - nu îţi vor mai putea trimite mesaje sau posta lucruri neplăcute;
- **strânge dovezi** - păstrează, prin salvare sau făcând o captură de ecran, e-mailurile, mesajele, imaginile, filmuleţele răutăcioase pe care le primeşti şi arată-le părinţilor;
- **gândește-te mereu la ceea ce publici on-line** - agresorii pot folosi ce ai postat împotriva ta, să transmită altora sau să râdă de tine. Şi nu posta tu nimic care ar putea răni sau jena pe altcineva;
- **nu aprecia şi nu transmite mai departe** mesajele sau postările în care cineva râde de o persoană sau spune lucruri urâte despre ea. Dacă faci asta, devii şi tu un agresor;
- **nu spune parolele de la conturile tale** - chiar și copiii care par prieteni ar putea să le folosească pentru a-ţi accesa conturile, să posteze lucruri neplăcute sau să transmită mesaje răuvoitoare în numele tău.

PAGINA PĂRINŢILOR

1. COMUNICAREA ESTE ESENŢIALĂ! Încurajează-ţi constant copilul să discute cu tine despre experienţele on-line şi lasă-l să înţeleagă că poate apela la tine pentru orice problemă, de fiecare dată când se întâmplă ceva care îl supără sau îl face să se simtă inconfortabil. Iar pentru "varianta de rezervă" (în ciuda deschiderii şi eforturilor noastre, celor mici le poate fi mai uşor să vorbească cu altcineva) spune-i că nu este nicio problemă dacă discută cu o persoană în care aveţi încredere amândoi (prieten, rudă, profesor) sau chiar sună la Telefonul Copilului 116 111.

2. "LASĂ CĂ ÎŢI TRECE!" NU ESTE O SOLUŢIE. Cyberbullying-ul îi poate face pe cei mici să se simtă ruşinaţi şi să se retragă în ei, având efecte reale de ordin psihic (supărare, furie), emoţional (apatie, pierderea interesului pentru lucrurile care le plac) şi chiar fizic (oboseală, insomnii), care în cazuri extreme pot ajunge până la suicid. Comunicând deschis şi acordând atenţia necesară cazurilor de hărţuire on-line, îţi poţi ajuta copilul să îşi recâştige încrederea şi sănătatea.

3. RAPORTEAZĂ, BLOCHEAZĂ, DOVEDEŞTE. Platformele de socializare (TikTok, Facebook, YouTube, Instagram, WhatsApp) permit blocarea şi raportarea userilor şi/sau a conţinutului şi comentariilor postate de aceştia. În situaţii de hărţuire on-line, fie realizezi împreună cu cel mic aceste procese, fie îl înveţi cum să raporteze şi blocheze singur agresorii şi mesajele lor. De asemenea, colectarea de dovezi (mesaje text și capturi de ecran ale postărilor de pe rețelele de socializare, inclusiv fișiere media), poate fi utilă pe termen lung, pentru a demonstra agresiunile.

4. MĂSURI DE PREVENŢIE. Pe cât posibil, monitorizează activitatea pe Internet a copilului, respectiv comentariile primite la ceea ce postează. Pentru protecţia lui, în conturile on-line setările de confidenţialitate trebuie să fie cele de cont privat, limitând doar la lista de prieteni publicul care poate vedea ceea ce postează şi care poate comenta sau transmite mesaje.

5. FEŢELE CYBERBULLYING-ULUI. Teama ca cel mic să devină o victimă a cyberbullying-ului este fondată în zilele noastre, însă nu uita că există şi rolurile de **agresor** sau **martor**. Copilul trebuie să înţeleagă că hărţuirea on-line nu este distractivă şi nu orice acţiune făcută sau orice cuvânt spus pe Internet poate intra la categoria "A fost o glumă!". Mesajul principal? Să se comporte cu ceilalţi la fel cum ar vrea ca alţii să se comporte cu el! Iar în cazul în care asistă la un caz de cyberbullying – indiferent dacă victima este o persoană cunoscută sau nu – să nu devină un martor complice încurajând comportamentul agresorului (prin distribuire, apreciere etc.), ci să fie un martor protector (sprijinirea victimei cu mesaje de susţinere, reclamarea hărţuirii/agresorului).

certSIGN

Cyber4Kids

LECŢIA 7.
WiFi sau nu?

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – BAGHETA ÎNCREDERII! Ea te va ajuta să te conectezi în siguranţă la Internet şi vei şti ce reţele sunt în regulă pentru tine!

1 **PE INTERNET, PRIN WIFI.** Pentru a intra pe Internet, trebuie doar să te conectezi on-line de pe telefon, tabletă sau calculator. Una din uşile pe care poţi intra în Internet este reţeaua WiFi. O foloseşti acasă, la şcoală sau din locuri publice – muzee, parcuri, restaurante, magazine, aeroporturi sau hoteluri. Însă, dacă la reţeaua WiFi de acasă te conectezi doar tu şi familia ta, la celelalte oricine poate avea acces. Inclusiv răufăcătorii on-line!

2 **CUM TE PROTEJEZI?** Respectând de fiecare dată aceste sfaturi:

• **Ai grijă la ce WiFi te conectezi.** Chiar dacă include denumirea locului în care te afli, asta nu înseamnă că acea reţea nu a fost făcută de un răufăcător şi nu este o capcană!

• **WiFi-urile publice pot să nu fie sigure.** Chiar dacă există o cheie - o parolă - pentru a le accesa, şi un infractor o cunoaşte. Poate fi chiar persoana de la masa de lângă tine, dintr-un restaurant, care va putea să vadă ce mesaje trimiţi, să îţi descopere parolele sau să îţi acceseze conturile.

• **Nu introduce date personale în site-uri, conectat de pe WiFi-uri publice.** Nu ştii cine poate să le vadă atunci când stai pe Internet folosind o conexiune care nu este sigură! Alte persoane din aceeaşi rețea pot vedea ce trimiţi și pot avea acces la informațiile tale personale, contacte, poze, nume de utilizator și parole.

• **Nu lăsa telefonul, tableta sau laptopul să se conecteze automat la WiFi.** Roagă-i pe părinţi să oprească această funcţie din dispozitivele tale.

• **Nu instala aplicaţii şi nu accesa site-uri şi linkuri necunoscute de pe WiFi-uri publice**. Asigură-te că linkurile pe care ai intrat au în faţa adresei un lacăt închis şi încep cu HTTPS.

PAGINA PĂRINȚILOR

1. WIFI PRIVAT, PUBLIC SAU CONEXIUNI MOBILE? Explică-i copilului principalele diferenţe dintre mijloacele de conectare la Internet: WiFi-ul privat, de acasă (plătit, securizat, care poate fi accesat doar de către voi prin introducerea unei parole secrete - nu şi de către vecini), WiFi-ul din locuri publice precum muzee, parcuri, restaurante, magazine, aeroporturi sau hoteluri (deschis pentru oricine care cunoaşte parola, atunci când aceasta există, şi nu la fel de sigur) şi datele mobile (conexiune pentru telefoane, tablete, plătită şi limitată, care poate genera costuri suplimentare).

2. RISCURILE REŢELELOR PUBLICE DE WIFI. Pentru ca cel mic să înţeleagă de la tine de ce nu este indicat să folosească reţele WiFi cu acces liber, trebuie mai întâi să ştii tu care sunt riscurile acestora:

• **Man-in-the-Middle (MitM)**. Un atac MitM presupune interceptarea unei comunicări între două sisteme, de către o terţă parte externă. Indiferent despre ce vorbim (e-mail, rețele de socializare, navigare pe Internet), infractorii cibernetici pot intercepta direct comunicarea atunci când te conectezi la o reţea WiFi necriptată, riscând alterarea mesajelor, furtul datelor personale, a informaţiilor de pe dispozitiv (parole, informaţii bancare etc.).

• **Malware**. Atacatorii te pot păcăli să descarci conținut de tip malware atunci când te conectezi la un WiFi public. Pericolul programelor malware (viruşi, viermi informatici, spyware, adware, troiani) poate varia de la infectarea dispozitivelor, furtul de informaţii personale, vizualizarea fişierelor off-line precum fotografii și documente sensibile, până la accesarea camerei și microfonului, astfel încât altcineva să ştie ce faci şi în lumea reală, nu doar on-line.

• **Hotspot-uri maliţioase.** Infractorii cibernetici pot seta un hotspot într-o zonă publică, denumindu-l “WiFi Public” sau după o cafenea, un magazin ori sediul unei firme din apropiere. Aflându-te în căutarea unei conexiuni gratuite la Internet, un astfel de nume îţi poate părea legitim şi poţi deveni uşor victima atacatorilor care îţi vor spiona activitatea on-line, fără să îţi dai seama că eşti în pericol.

3. SSL ŞI VPN LA PUTERE! Mai ales pe WiFi-uri publice, trebuie utilizate conexiuni SSL (adică trebuie accesate doar acele site-uri care includ la începutul linkurilor un lacăt închis şi **HTTPS**). Acest protocol presupune criptarea traficului dintre dispozitivul tău și un site web, garantând autenticitatea celui din urmă şi făcând dificilă interceptarea comunicaţiilor de către intruși.

De asemenea, este indicat să foloseşti pe toate dispozitivele o soluţie **VPN** (Virtual Private Network) pentru securizarea activităţii pe Internet, criptarea traficului şi ascunderea adresei IP. Conexiunea sigură între tine și Internet creată de această rețea virtuală privată este esenţială pentru protejarea datelor personale în mediul on-line.

certSIGN

Cyber4Kids

LECŢIA 8.
Parole magice

Urmând aceste sfaturi de securitate cibernetică vei deveni un Super Cyber-Erou şi vei activa un obiect magic – CUFĂRUL ÎNŢELEPCIUNII! În el poţi păstra în siguranţă parole mega-puternice, pe care niciun infractor nu le va descoperi!

1. **PAROLE PUTERNICE.** Nu folosi în parole cuvinte simple (ex. Minecraft, ciocolata, StarWars) ori numere consecutive (123456). Şi NU, cuvântul "parolă" nu este deloc o parolă bună! O parolă puternică trebuie să fie mai lungă - de cel puţin 8 caractere - şi mai complicată. Amestecă în ea litere mari şi litere mici, cifre şi simboluri.

2. **PAROLE AMUZANTE.** Scoate primele litere ale fiecărui cuvânt dintr-o propoziţie amuzantă creată de tine, pe care să o reţii uşor, şi introdu numere şi simboluri. De exemplu, din propoziţia "Iepurele şi pisica au văzut două filme la Cinema" vei obţine această super parolă - **I&pav2f@C**.

3. **FĂRĂ DATE PERSONALE.** Nu include în parole numele tău, data naşterii, numele părinţilor, numărul de telefon sau orice alte date personale pe care le-ar putea şti ori ghici şi alţii.

4. **PAROLE SECRETE.** Nu spune nimănui parolele tale, cu excepţia părinţilor! Şi cei mai buni prieteni ar putea fi tentaţi să facă o glumă pe seama ta şi să le folosească pentru a-ţi accesa conturile, pretinzând că eşti tu. Şi nu nota niciodată parolele într-un loc uşor de găsit de către altcineva (caiete, post-it-uri etc.).

5. **PAROLE DIFERITE.** Nu folosi aceeaşi parolă peste tot! Este bine să ai una diferită pentru fiecare cont (jocuri, Facebook, YouTube Instagram, TikTok, e-mail). Folosirea aceleiași parole pentru mai multe conturi este ca și cum ai avea o cheie pentru toate ușile. Dacă un răufăcător fură sau copiază cheia, toate sunt vulnerabile.

PAGINA PĂRINŢILOR

1. "CEI 3 PURCELUŞI", VARIANTA PAROLE. Pentru a înţelege mai bine diferenţele între o parolă slabă, una medie şi una puternică, respectiv importanţa celei din urmă, îi poţi explica copilului aceste lucruri folosindu-te de reinterpretarea unei poveşti (a unui film sau situaţii din viaţa reală, ţine de inspiraţia şi imaginaţia ta). Noi propunem "Cei trei purceluşi", în care lupul devine infractorul cibernetic iar cele trei case construite devin:

• **parola slabă** (casa din paie) – extrem de uşor de spart sau de ghicit. Exemple: parola123, qwerty, andrei111;

• **parola medie** (casa din nuiele) – un grad mai ridicat de dificultate, însă nu imposibil de ghicit, indiferent că vorbim despre persoane care îl cunosc pe copil sau despre soft-uri maliţioase (keylogger, screen scraper) utilizate de criminalii cibernetici. Exemple: Andrei2o2o, ImiPlaceLego;

• **parola puternică** (casa din piatră şi cărămidă) – un grad ridicat de dificultate, permiţând păstrarea conturilor şi a informaţiilor personale în siguranţă. Exemple: Ipsm@C&svHP, DCv1L&3cJup.

2. JOCUL PAROLELOR MAGICE. Transformă crearea unor parole puternice (mai multe, diferite pentru fiecare cont) într-un joc pe care să îl realizaţi împreună periodic – parolele ar trebui schimbate măcar o dată la fiecare 6 luni. Lasă-l pe copil să vină cu idei de propoziţii simple şi amuzante, pe care el să le poată reţine uşor, iar apoi îndrumă-l cum să obţină parole puternice prin extragerea primei litere a fiecărui cuvânt şi inserarea de cifre şi simboluri.

Exemplele de mai sus le-am obţinut din propoziţiile "Îmi place să merg la Cinema şi să văd Harry Potter" (Ipsm@C&svHP) şi "De Crăciun vreau un Lego şi trei cărţi Jurnalul unui puşti" (DCv1L&3cJup). Iar de Paşti schimbaţi parolele!

3. DAR E PAROLA MEA! Este foarte posibil ca cel mic să nu înţeleagă de ce ar trebui să îi ştii parolele (doar sunt secrete, nu?) sau să nu fie tocmai încântat de faptul că vei avea acces la activitatea lui on-line. Fă-l să înţeleagă că siguranţa lui, inclusiv în mediul virtual, este datoria ta de părinte.

Iar faptul că vei avea parolele de la conturile lui nu înseamnă că le vei folosi pentru a urmări fiecare lucru pe care îl face pe Internet. De altfel, chiar şi acasă, copilul poate ţine închisă uşa de la camera lui iar tu să baţi înainte de a intra. Însă nu este admisibil ca tu, părinte, să nu ai acces.

certSIGN

Cyber4Kids

Video

Bine ai venit în Cyber City!
(ep. 0) | [EN Sub]

Ne jucam în siguranţă
(ep.1) | [EN Sub]

Date personale secrete
(ep.2) | [EN Sub]

Cine te păcăleşte online
(ep.3) | [EN Sub]

Linkuri periculoase
(ep.4) | [EN Sub]

Internetul nu uită
(ep.5) | [EN Sub]

Cyberbullying
(ep.6) | [EN Sub]

WiFi sau nu?
(ep.7) | [EN Sub]

Parole magice
(ep.8) | [EN Sub]

youtube.com/certsign