CYBERSHIELD
ASOCIATIA EDUCATIE IN SECURITATE CIBERNETICA

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

GHID PRACTIC · EDIȚIA 2026

Ghidul de securitate cibernetică pentru cadrele didactice

Protejează-ți identitatea digitală, reputația școlii și datele elevilor.

Amenințări explicate pe înțelesul tuturor, măsuri de prevenție, proceduri pas-cu-pas și liste de verificare gata de tipărit.

Elaborat de **Asociația Educație în Securitate Cibernetică – CyberShield**
cu sprijinul **Directoratului Național de Securitate Cibernetică (D.N.S.C.)**

Document gratuit — destinat distribuirii în unitățile de învățământ

Cuprins

1 Introducere: de ce este importantă securitatea pentru cadrele didactice

Securitatea cibernetică nu mai este o problemă „a informaticienilor". Pentru un cadru didactic din 2026, ea este parte din igiena profesională de zi cu zi — la fel de firească precum verificarea catalogului sau pregătirea lecției.

Cadrul didactic de azi lucrează aproape permanent online: trimite și primește e-mailuri, gestionează clase în Google Classroom sau Microsoft Teams, comunică în grupuri de WhatsApp cu părinții și elevii, introduce note și absențe în catalogul electronic și își menține o prezență pe rețelele sociale. Fiecare dintre aceste activități, oricât de banală pare, deschide o ușă pe care un atacator o poate folosi.

Vestea bună este că marea majoritate a atacurilor nu reușesc datorită unei tehnologii sofisticate, ci datorită unei greșeli umane simple: o parolă slabă, un click pe un link fals, o aplicație lăsată conectată pe un calculator din cancelarie. Asta înseamnă că **cele mai multe atacuri pot fi prevenite cu măsuri simple**, pe care le poți aplica imediat, fără cunoștințe tehnice avansate.

> **Cui se adresează acest ghid**
>
> Tuturor cadrelor didactice — învățători, profesori, diriginți, directori, personal auxiliar — indiferent de nivelul de cunoștințe tehnice. Nu trebuie să fii expert. Trebuie doar să adopți câteva obiceiuri sănătoase și să știi cum să reacționezi când ceva pare în neregulă.

Cum este structurat ghidul

Capitolele 2–4 te ajută să înțelegi **de ce** și **cum** ești atacat. Capitolul 5 tratează fiecare amenințare după aceeași schemă: *ce este · cum arată în realitate · cum o previi · ce faci dacă ai căzut victimă*. Capitolele 6–8 sunt despre prevenție și instrumentele tale zilnice. Capitolele 9–10 explică **unde raportezi** și ce faci concret într-un incident. La final ai mituri demontate, liste de verificare gata de tipărit, contacte oficiale și un glosar.

> **Două adrese de reținut din start**
>
> **Ai văzut ceva suspect** (un site fals, un mesaj de phishing, o tentativă de fraudă)? Raportează la **cyberskill.ro**, secțiunea **Raportează**.
> **Ai căzut victimă unui incident**? Raportează la **pnrisc.dnsc.ro** și sună la **1911**.

> *„Un profesor protejat nu se apără doar pe sine. Protejează indirect zeci de elevi, familiile lor și reputația întregii școli."*

2 De ce cadrul didactic este o țintă

Cadrele didactice sunt printre cele mai expuse categorii profesionale din mediul online — nu pentru că ar fi neglijente, ci pentru combinația dintre volumul de date pe care le gestionează și accesul larg la platforme.

Expunere mare, în continuă creștere

Digitalizarea învățământului a adus enorme beneficii, dar a mărit și „suprafața de atac": fiecare cont nou, fiecare aplicație, fiecare grup online este o nouă posibilă breșă. Amenințările evoluează rapid — tehnicile de înșelăciune de acum un an sunt deja depășite de altele mai convingătoare, generate uneori cu inteligență artificială. **A ține pasul nu este opțional: este o responsabilitate continuă.**

Datele pe care le gestionezi sunt valoroase

Un cadru didactic are acces, direct sau indirect, la o cantitate surprinzătoare de date sensibile: nume, adrese, CNP-uri, note, situații medicale sau familiale ale elevilor minori, date de contact ale părinților, informații despre colegi. Pentru un atacator, aceste date înseamnă bani — prin șantaj, fraudă de identitate sau revânzare.

Cadrul didactic este o „cheie" către mulți alții

Contul unui cadru didactic este o poartă către părinți, elevi și colegi. Dacă atacatorul preia contul tău, poate trimite mesaje credibile către zeci de oameni care au încredere în tine — exact de asta ești o țintă atât de atractivă.

Cele trei victime ale unui singur incident

Cine are de suferit	Cum este afectat
Cadrul didactic	Pierderea accesului la conturi, furtul identității, mesaje frauduloase trimise în numele tău, prejudiciu de imagine, stres și timp pierdut pentru recuperare.
Școala	Reputația instituției afectată, pierderea încrederii părinților, posibile sancțiuni pentru încălcarea protecției datelor, perturbarea activității.
Elevii, părinții, colegii	Expunerea datelor personale ale minorilor, escrocherii direcționate către părinți („profesorul cere bani"), compromiterea altor conturi prin efect de domino.

De reținut

Datele elevilor sunt date ale unor **minori**. Responsabilitatea legală și morală de a le proteja este semnificativ mai mare decât în cazul datelor obișnuite.

3 Suprafața ta de expunere: unde ești vulnerabil

Înainte de a te apăra, trebuie să știi exact pe unde poți fi atacat. Iată „hărțile" tale digitale — locurile pe care le folosești zilnic și riscurile asociate fiecăruia.

E-mailul profesional și personal

E-mailul este poarta principală de intrare. Prin el primești tentativele de phishing, prin el se resetează parolele celorlalte conturi, iar dacă este compromis, atacatorul poate ajunge la tot restul. Riscuri tipice: mesaje false „de la conducere" sau „de la inspectorat", atașamente infectate, linkuri către pagini de autentificare clonate.

Google Classroom / Microsoft Teams

Platformele de învățare conțin teme, note, comentarii și uneori date personale ale elevilor. Riscuri: linkuri de invitație distribuite public (intruși în clasă), elevi care preiau controlul prin conturi nesecurizate, partajarea accidentală a materialelor sau a ecranului cu informații sensibile.

Grupurile de WhatsApp cu părinți și elevi

Foarte comode, dar și foarte riscante. Într-un grup, numărul tău de telefon devine vizibil pentru toți membrii. Circulă mesaje virale, linkuri de tip „felicitări, ați câștigat", colecte de bani și, ocazional, tentative de impersonare. Confidențialitatea elevilor poate fi încălcată ușor prin fotografii sau informații distribuite necontrolat.

Catalogul electronic / virtual

Conține exact tipul de date pe care un atacator și le dorește: note, absențe, date de identificare ale elevilor. Riscuri: parole slabe sau refolosite, autentificare de pe calculatoare partajate fără deconectare, sesiuni lăsate deschise în cancelarie, dispozitive personale neprotejate.

Rețelele sociale

Ce postezi public spune mult despre tine — locul de muncă, programul, locația, familia. Aceste informații alimentează atacurile de „inginerie socială", în care escrocul pare să te cunoască. Conturile de Facebook ale cadrelor didactice sunt frecvent clonate pentru a păcăli contactele.

Dispozitivele: laptop, telefon, calculator

Un dispozitiv fără ecran blocat, fără actualizări, cu aplicații conectate permanent, este o vulnerabilitate ambulantă. Calculatoarele partajate din școală sunt un caz special: oricine se poate așeza după tine la tastatură.

> **Exercițiu de 5 minute: harta ta de expunere**
>
> Notează toate conturile și platformele pe care le folosești pentru muncă. Pentru fiecare, întreabă-te: *Are parolă unică? Are autentificare în doi pași? Cine altcineva are acces? De pe ce dispozitive mă conectez?* Vei vedea imediat unde ești cel mai vulnerabil și de unde să începi.

4 Cum gândește un atacator: anatomia unui atac

Atacurile nu sunt magie. Aproape toate urmează aceiași pași. Dacă îi recunoști, poți întrerupe lanțul devreme — și atunci atacul eșuează.

Etapă	Ce face atacatorul	Unde îl poți opri
1. Recunoaștere	Strânge informații despre tine din rețele sociale, site-ul școlii, grupuri publice.	Limitează ce publici; setează profilurile pe privat.
2. Momeala	Trimite un mesaj credibil (e-mail, SMS, mesaj în grup) care creează urgență.	Recunoaște semnalele de phishing; nu acționa sub presiune.
3. Capcana	Te duce pe o pagină falsă sau te face să deschizi un atașament.	Verifică adresa; nu introduce parola pe linkuri din mesaje.
4. Compromiterea	Îți fură parola sau infectează dispozitivul.	2FA blochează intrarea chiar dacă parola e furată.
5. Exploatarea	Folosește contul tău: fraudă, furt de date, mesaje către contactele tale.	Detectează rapid (notificări) și reacționează (capitolul 10).

Exemplu de lanț complet

1. Atacatorul vede pe Facebook că ești dirigintă la o anumită școală.
2. Îți trimite un e-mail „de la secretariatul școlii", cu un subiect urgent.
3. Linkul duce la o pagină Google falsă.
4. Introduci parola — el o capturează.
5. A doua zi, părinții din grup primesc un mesaj „de la tine" care cere o colectă urgentă.

O singură verificare la pasul 2 sau 3 ar fi oprit totul.

Concluzia

Nu trebuie să fii perfect la toate etapele. Este suficient să întrerupi *una* singură. De aceea măsurile mici (2FA, verificarea unui link) au impact uriaș.

5 Amenințările: ce sunt, cum le previi, ce faci dacă ai căzut victimă

Fiecare amenințare este tratată după aceeași schemă, ca să o poți folosi rapid: **ce este**, **cum arată în realitate** (exemplu), **cum o previi** și **ce faci dacă ai căzut victimă**.

Două reguli valabile la toate amenințările

Prevenție: dacă vezi ceva suspect, raportează-l la **cyberskill.ro → secțiunea Raportează**, ca să-i protejezi și pe ceilalți.
Dacă ai căzut victimă: raportează incidentul la **pnrisc.dnsc.ro** și sună la **1911** (DNSC).

AMENINȚAREA #1

Phishing prin e-mail (mesaje-momeală)

Mesaje care imită o sursă de încredere (Google, banca, inspectoratul, conducerea școlii) ca să te convingă să dai click, să introduci parola sau să deschizi un atașament.

Cum arată: „Contul tău Google va fi dezactivat în 24 de ore. Confirmă-ți identitatea aici." Expeditor: *support@gooogle-verify.com*. Linkul duce la o pagină identică cu cea reală.

Cum o previi

Verifică adresa expeditorului și linkul (treci cu mouse-ul peste el). Nu acționa sub presiune de timp. Când pare de la o instituție, contacteaz-o separat, pe un canal oficial. **Raportează mesajul la cyberskill.ro → Raportează.**

Dacă ai căzut victimă

Schimbă imediat parola (de pe alt dispozitiv), activează 2FA, verifică regulile de redirecționare a e-mailului. Raportează la **pnrisc.dnsc.ro / 1911**.

AMENINȚAREA #2

Smishing și Vishing (SMS și apeluri false)

Aceeași momeală, livrată prin SMS (*smishing*) sau prin apel telefonic (*vishing*). Tot mai des, vocea poate fi generată cu AI.

> **Cum arată:** SMS „Coletul tău nu a putut fi livrat, plătește 2 lei taxă: [link]." Sau un apel: „Bună ziua, sunt de la bancă, am detectat o tranzacție suspectă, confirmați codul primit prin SMS."

Cum o previi

> Nu da click pe linkuri din SMS neașteptate. Nicio instituție serioasă nu cere coduri sau parole la telefon. Închide și sună tu, la numărul oficial. **Raportează la cyberskill.ro → Raportează.**

Dacă ai căzut victimă

> Sună imediat banca dacă ai dat date financiare; schimbă parolele afectate; raportează la **pnrisc.dnsc.ro / 1911** și, dacă ai pierdut bani, depune plângere la cea mai apropiată secție de poliție.

AMENINȚAREA #3

Conturi compromise și parole slabe

Atacatorul ghicește, fură sau cumpără parola și intră în cont. Cel mai mare risc: **refolosirea aceleiași parole** pe mai multe conturi.

> **Cum arată:** primești o notificare „Conectare nouă din [oraș necunoscut]" sau parola „nu mai merge" brusc. Prietenii primesc mesaje pe care nu le-ai trimis.

Cum o previi

> Parolă unică pentru fiecare cont + manager de parole + autentificare în doi pași (vezi capitolul 6).

Dacă ai căzut victimă

> Schimbă parola de pe un dispozitiv sigur, deconectează toate sesiunile, activează 2FA, verifică ce alte conturi foloseau aceeași parolă. Raportează la **pnrisc.dnsc.ro / 1911**.

AMENINȚAREA #4

Furt de identitate și impersonare

Cineva se dă drept tine — îți clonează contul de Facebook, îți copiază poza și numele, scrie părinților sau colegilor în numele tău.

> **Cum arată:** apare un al doilea profil cu numele și poza ta, care trimite cereri de prietenie contactelor tale și apoi mesaje de tip „am o urgență, poți să-mi trimiți...".

Cum o previi

> Setează profilul pe privat și limitează cine îți vede lista de prieteni și pozele. Dacă cineva te clonează, **raportează contul fals direct în platformă** (Facebook/Instagram) și roagă-ți prietenii și cunoștințele să raporteze și ei contul-clonă — mai multe raportări duc la eliminarea lui mai rapidă.

Dacă ai căzut victimă

> Raportează contul fals direct în platformă (Facebook/Instagram) și roagă-ți prietenii și cunoștințele să-l raporteze și ei — mai multe sesizări duc la eliminarea lui mai rapidă. Anunță-ți public contactele să nu reacționeze și securizează-ți contul real (parolă nouă + 2FA). Vezi și capitolul 15.

AMENINȚAREA #5

Frauda „de la director / inspectorat" (compromiterea comunicării)

Un mesaj care pare de la o autoritate din școală îți cere urgent ceva: să plătești o factură, să cumperi vouchere, să trimiți o listă cu date ale elevilor.

> **Cum arată:** „Sunt directorul, sunt într-o ședință și nu pot vorbi. Am nevoie urgent să cumperi 3 vouchere și să-mi trimiți codurile. Îți decontez azi." — de pe un număr/e-mail necunoscut.

Cum o previi

> Regula de aur: **verifică pe alt canal**. Sună persoana real, direct. Autoritatea + urgența + secretul sunt semnalul clasic de fraudă. **Raportează tentativa la cyberskill.ro → Raportează.**

Dacă ai căzut victimă

> Anunță imediat conducerea reală a școlii; dacă ai trimis bani, anunță imediat banca și depune plângere la cea mai apropiată secție de poliție; raportează la **pnrisc.dnsc.ro / 1911**.

AMENINȚAREA #6

Malware și ransomware

Programe dăunătoare care ajung pe dispozitiv prin atașamente, linkuri sau stick-uri USB. *Ransomware* îți criptează fișierele și cere bani pentru deblocare.

> **Cum arată:** deschizi un atașament „Factura.docx" și, după o vreme, fișierele tale didactice nu se mai deschid; apare un mesaj care cere plată pentru deblocare.

Cum o previi

> Nu deschide atașamente neașteptate; ține sistemul și antivirusul la zi; nu introduce stick-uri necunoscute; fă **backup** regulat (capitolul 6).

Dacă ai căzut victimă

> Deconectează dispozitivul de la rețea, nu plăti răscumpărarea, cere ajutor specializat și raportează la **pnrisc.dnsc.ro / 1911**. Restaurează din backup.

AMENINȚAREA #7

Inginerie socială

Manipulare psihologică: atacatorul folosește informații reale despre tine ca să pară credibil și să te determine să faci o greșeală.

> **Cum arată:** cineva te sună și „știe" numele școlii, al directorului și clasa ta, apoi cere o „confirmare rapidă" a unor date — exact pentru că pare să te cunoască, lași garda jos.

Cum o previi

> Faptul că cineva știe detalii despre tine nu îl face de încredere. Verifică identitatea pe un canal separat. Limitează informațiile publicate online.

Dacă ai căzut victimă

> Schimbă ce date/parole ai dezvăluit; anunță persoanele/instituțiile afectate; raportează la **pnrisc.dnsc.ro / 1911**.

AMENINȚAREA #8

Deepfake și conținut generat de AI

Imagini, voci sau clipuri false, generate de inteligență artificială, care par autentice. Pot fi folosite pentru escrocherii vocale sau pentru a-ți atribui fals afirmații.

Cum arată: un mesaj vocal „de la un coleg" cu vocea lui, care cere bani urgent; sau un clip trucat în care pari că spui ceva ce nu ai spus.

Cum o previi

Tratează cu scepticism conținutul șocant sau urgent. Confirmă pe alt canal înainte de a reacționa sau a distribui. Nu redistribui materiale neverificate.

Dacă ai căzut victimă

Păstrează dovezile (capturi, fișiere), anunță persoanele vizate, raportează la **cyberskill.ro → Raportează** și la **pnrisc.dnsc.ro / 1911**; dacă e defăimare, depune plângere la cea mai apropiată secție de poliție.

AMENINȚAREA #9

Wi-Fi public și rețele nesecurizate

Rețelele deschise (cafenele, aeroporturi, uneori rețele de școală prost configurate) pot fi folosite pentru a-ți intercepta traficul sau a te direcționa către pagini false.

Cum arată: te conectezi la „Free_WiFi", iar o pagină îți cere să te „autentifici cu contul Google" — în realitate o capcană de colectare a parolelor.

Cum o previi

Evită autentificarea în conturi sensibile (catalog, e-mail, bancă) pe Wi-Fi public. Folosește datele mobile sau o conexiune de încredere.

Dacă ai căzut victimă

Schimbă parolele introduse pe rețeaua respectivă; activează 2FA; raportează la **pnrisc.dnsc.ro / 1911**.

AMENINȚAREA #10

Oversharing și expunerea datelor

Publicarea prea multor detalii personale și profesionale, care devin „materie primă" pentru atacuri. Include și postarea de fotografii cu elevi fără acordul părinților.

Cum arată: postezi public locul de muncă, programul, poze din clasă cu elevi identificabili — informații care ajută atât escrocii, cât și încalcă confidențialitatea minorilor.

Cum o previi

Profiluri pe privat; gândește înainte de a posta; nu publica fotografii cu minori fără consimțământ (vezi capitolul 10).

Dacă ai căzut victimă

Șterge conținutul expus, cere eliminarea lui unde a fost redistribuit; dacă sunt implicate date ale elevilor, anunță conducerea școlii și DPO-ul.

6 Regulile de igienă cibernetică (prevenție)

„Igiena cibernetică" înseamnă obiceiurile simple și repetate care te țin în siguranță — la fel cum spălatul pe mâini previne bolile. Iată setul esențial, explicat pe pași.

1. Parole puternice și unice

O parolă bună este **lungă** (minimum 12–14 caractere), **unică** pentru fiecare cont și ușor de ținut minte de tine, dar greu de ghicit de alții. Metoda „fraza de acces": patru cuvinte fără legătură, de exemplu *Catalog-Munte-Verde-7Cafele*.

Nu face niciodată

Nu folosi aceeași parolă pe mai multe conturi. Nu folosi date evidente (numele, data nașterii, „parola123"). Nu nota parolele pe bilețele lipite de monitor.

2. Manager de parole

Este imposibil să ții minte zeci de parole unice — și nici nu trebuie. Un manager de parole le generează, le stochează criptat și le completează automat. Tu reții o singură parolă-cheie. Există opțiuni gratuite și de încredere.

3. Autentificarea în doi pași (2FA)

Cea mai eficientă măsură unică pe care o poți lua. Pe lângă parolă, contul cere un al doilea cod (din aplicație sau SMS). Chiar dacă cineva îți află parola, nu poate intra fără al doilea pas.

Activează autentificarea în mai mulți pași în această ordine de prioritate

1. E-mailul — cheia tuturor conturilor.
2. Conturile Google / Microsoft.
3. Facebook și rețelele sociale.
4. Catalogul electronic, dacă oferă opțiunea.
5. Orice alt cont important.

4. Actualizări la zi

Actualizările repară fix vulnerabilitățile pe care le exploatează atacatorii. Activează actualizările automate pentru sistemul de operare, browser și aplicații.

5. Backup (copii de rezervă)

Regula simplă: dacă un fișier există într-un singur loc, deja l-ai pierdut. Ține copii ale materialelor importante în **două locuri** (de exemplu, cloud + un stick/hard extern). Astfel, un ransomware sau un dispozitiv stricat nu îți distruge munca.

6. Separarea conturilor personale de cele profesionale

Folosește conturi diferite pentru muncă și pentru viața personală. Dacă unul este compromis, celălalt rămâne protejat, iar datele elevilor nu se amestecă cu cele personale.

7. Securizarea dispozitivelor

Blochează ecranul cu PIN, amprentă sau parolă, pe telefon și laptop. Setează blocarea automată după câteva minute. Pe calculatoarele partajate din școală, **deconectează-ți întotdeauna conturile** la final (ieși din cont, nu doar închide fereastra).

8. Navigare și click în siguranță

Verifică adresa unui site înainte de a introduce date. Nu da click pe linkuri din mesaje neașteptate. Treci cu mouse-ul peste link ca să vezi unde duce de fapt. Când ai cea mai mică îndoială — oprește-te.

> **Prevenția înseamnă și să raportezi**
>
> De fiecare dată când întâlnești un mesaj de phishing, un site fals sau o tentativă de fraudă, **raportează-l la cyberskill.ro → secțiunea Raportează**. Astfel ajuți la avertizarea altor cadre didactice și a altor școli — prevenția este un efort colectiv.

> **Cele 3 reguli de aur, dacă reții doar atât**
>
> **1.** Parolă unică + manager de parole. **2.** Autentificare în doi pași peste tot. **3.** Gândește înainte de a da click.

7 Autentificarea în doi pași, pas cu pas

Autentificarea în doi pași (2FA) este cea mai eficientă măsură unică pe care o poți lua. Iată cum o activezi pe cele mai importante conturi. Pașii pot diferi ușor în funcție de versiunea aplicației, dar logica este aceeași.

Ce metodă să alegi

O **aplicație de autentificare** (care generează coduri) este mai sigură decât codul prin SMS, fiindcă SMS-ul poate fi interceptat. Dacă platforma permite, alege aplicația de autentificare. Oricare variantă de 2FA este însă infinit mai bună decât niciuna.

Cont Google (Gmail, Classroom, Drive)

1. Intră în **Contul Google** → **Securitate**.
2. Alege **Verificarea în doi pași** și apasă „Începe".
3. Confirmă parola și alege metoda: aplicație de autentificare (recomandat), notificare pe telefon sau SMS.
4. Salvează **codurile de rezervă** într-un loc sigur — îți permit accesul dacă pierzi telefonul.

Facebook

1. Intră în **Setări și confidențialitate** → **Securitate și autentificare**.
2. Deschide **Autentificarea cu doi factori** și apasă „Editează".
3. Alege aplicația de autentificare (recomandat) sau SMS și urmează pașii.

După activare

Verifică periodic, în setările de securitate, lista de **dispozitive conectate** și deconectează-le pe cele necunoscute. Păstrează codurile de rezervă într-un loc sigur (de exemplu, în managerul de parole).

Atenție la „oboseala de notificări"

Dacă primești o cerere de confirmare 2FA pe care nu ai inițiat-o tu, **nu o aproba** — înseamnă că cineva îți știe parola și încearcă să intre. Schimbă parola imediat.

8 Securitatea pe telefonul mobil

Telefonul a devenit principalul tău instrument de lucru: e-mail, catalog, WhatsApp, aplicații de școală. Dacă ajunge pe mâini greșite sau e infectat, expune tot. Iată regulile esențiale.

Blochează și protejează accesul

- Folosește un **PIN**, amprentă sau recunoaștere facială — nu un model simplu.
- Setează **blocarea automată** după 1–2 minute de inactivitate.
- Nu lăsa telefonul deblocat și nesupravegheat, mai ales în cancelarie sau la clasă.

Ține-l curat și actualizat

- Instalează **actualizările** de sistem și de aplicații imediat ce apar — repară vulnerabilități.
- Instalează aplicații **doar din magazinele oficiale** (Google Play, App Store).
- Verifică **permisiunile** aplicațiilor: o aplicație de lanternă nu are nevoie de contacte sau microfon.
- Dezinstalează aplicațiile pe care nu le mai folosești.

Pregătește-te pentru pierdere sau furt

- Activează funcția **„Găsește dispozitivul"** (Find My Device / Find My) pentru localizare și ștergere de la distanță.
- Fă **backup** automat al pozelor și documentelor importante.
- Învață cum blochezi/ștergi telefonul de la distanță dacă îl pierzi.

Atenție la capcanele mobile

- Nu da click pe linkuri din SMS sau WhatsApp neașteptate (smishing).
- Evită conturile sensibile pe Wi-Fi public; ține Bluetooth-ul oprit când nu îl folosești.
- Nu încărca telefonul în stații USB publice necunoscute.

> **Verificare rapidă**
>
> Telefon blocat automat? Da. Actualizări la zi? Da. „Găsește dispozitivul" activat? Da. Backup pornit? Da. — Dacă ai bifat toate, ești deja peste media de protecție.

9 Instrumentele de zi cu zi, în siguranță

Regulile generale aplicate concret pe cele trei instrumente pe care un cadru didactic le folosește cel mai des: platforma de clasă, grupul de WhatsApp și catalogul electronic.

Google Classroom / Microsoft Teams

- Nu distribui public linkul/codul clasei; trimite-l doar elevilor tăi și reînnoiește-l dacă a ajuns unde nu trebuia.
- Activează „sala de așteptare" / aprobarea participanților, ca să eviți intrușii.
- Atenție la partajarea ecranului — închide întâi e-mailul, catalogul și ferestrele cu date personale.
- Verifică periodic cine are acces la clasă și la materiale; elimină conturile care nu mai aparțin clasei.
- Folosește contul instituțional, cu 2FA activat, nu un cont personal.

Exemplu de greșeală frecventă

Un cadru didactic postează codul clasei pe pagina publică de Facebook a școlii. În scurt timp, persoane străine intră în clasă și o perturbă. *Soluție:* cod privat, doar pentru elevi, și aprobarea participanților activată.

Grupurile de WhatsApp cu părinți și elevi

- Stabilește de la început reguli clare ale grupului (scop, ce se postează, ore de liniște).
- Conștientizează că **numărul tău de telefon devine vizibil** tuturor; pentru anunțuri, folosește un grup în care scrie doar adminul.
- Nu posta fotografii cu elevi, note sau date personale ale minorilor în grup.
- Tratează cu suspiciune mesajele „urgente" despre bani, colecte sau linkuri-premiu — chiar dacă par de la un coleg.
- Dacă un membru pare să te impersoneze sau un cont se comportă ciudat, anunță grupul și verifică pe alt canal.

Capcana clasică

„Bună ziua, sunt doamna dirigintă, am rămas fără credit, puteți transfera urgent...". Niciodată nu acționezi pe baza unui mesaj urgent fără să confirmi telefonic, direct.

Catalogul electronic / virtual

- Folosește o parolă unică și puternică, diferită de cea de la e-mail sau Facebook.
- Activează autentificarea în doi pași dacă platforma o oferă.
- Accesează catalogul doar de pe dispozitive de încredere; evită Wi-Fi-ul public.
- Pe calculatoarele partajate, **deconectează-te complet** la final — nu doar închide fila.

- Nu salva parola catalogului în browserul unui calculator comun.
- Nu lăsa sesiunea deschisă și nesupravegheată în cancelarie.

> **Principiul comun**
>
> Indiferent de instrument, aceleași trei idei te protejează: **cont securizat** (parolă unică + 2FA), **acces controlat** (cine vede ce), **minimul de date expuse** (nu publica ce nu e necesar).

10 Protecția datelor elevilor

Regulamentul general privind protecția datelor (GDPR) nu este doar birocrație. Pentru un cadru didactic, acesta este reperul care îți spune cum să tratezi cu grijă datele unor minori aflați în responsabilitatea ta.

Principiile pe care le poți reține ușor

Principiu	În practică, pentru tine
Minimizarea datelor	Colectează și păstrează doar ce ai nevoie. Nu strânge date „pentru orice eventualitate".
Scopul precis	Folosește datele elevilor doar pentru activitatea didactică, nu pentru alte scopuri.
Securitate	Protejează datele prin parole, acces limitat și dispozitive securizate.
Consimțământ	Pentru fotografii, filmări sau publicarea de informații despre minori, este nevoie de acordul părinților.

Reguli concrete în activitatea zilnică

- Nu trimite liste cu date personale ale elevilor pe canale nesecurizate (grupuri de WhatsApp, e-mail personal).
- Nu publica fotografii cu elevi pe rețelele sociale fără consimțământul părinților.
- Nu lăsa documente cu date ale elevilor accesibile pe calculatoare partajate.
- Când nu mai ai nevoie de un document cu date personale, șterge-l/distruge-l corect.
- Raportează conducerii școlii orice scurgere sau pierdere de date — există termene legale de notificare.

Important

O breșă care expune datele elevilor poate atrage obligații legale de notificare și sancțiuni pentru școală. Anunță imediat conducerea și responsabilul cu protecția datelor (DPO), dacă există.

11 Securitatea acasă și în familie

Munca cadrului didactic nu se oprește la poarta școlii. Multe lecții, comunicări și accesări de catalog se fac de acasă — iar dispozitivele și rețeaua de acasă fac parte din aceeași suprafață de expunere.

Rețeaua de acasă (routerul Wi-Fi)

- Schimbă parola implicită a routerului (cea din fabrică, scrisă pe etichetă).
- Folosește o parolă puternică pentru rețeaua Wi-Fi și criptare modernă (WPA2/WPA3).
- Actualizează routerul dacă producătorul oferă actualizări.
- Creează o rețea separată „pentru oaspeți" pentru vizitatori și dispozitivele mai puțin sigure.

Calculatorul de acasă

- Conturi separate pentru fiecare membru al familiei; nu lucra din contul de administrator.
- Ține un cont distinct pentru activitatea didactică, separat de cel personal.
- Actualizări automate, antivirus activ, ecran blocat când te ridici.

Copiii și familia

- Activează controlul parental și discută deschis cu copiii despre riscurile online.
- Avertizează membrii familiei despre phishing și escrocherii — atacatorii vizează adesea ruda mai puțin atentă.
- Nu refolosi între membrii familiei aceleași parole sau conturi.

> **Cadrul didactic ca model**
>
> Obiceiurile tale digitale sănătoase îi influențează pe elevii și pe copiii tăi. Când aplici aceste reguli acasă, predai prin exemplu cea mai bună lecție de siguranță online.

12 Pentru directori: o cultură de securitate în școală

Securitatea unei școli este atât de puternică pe cât este cel mai vulnerabil cont. Conducerea poate transforma măsurile individuale într-o cultură comună, mult mai rezistentă.

Politici simple și clare

- Reguli scrise, scurte, despre parole, 2FA, gestionarea datelor elevilor și folosirea calculatoarelor comune.
- Un responsabil cu protecția datelor (DPO) și o persoană de contact pentru incidente.
- Formare periodică: sesiuni scurte de conștientizare pentru tot personalul.

Gestionarea conturilor și a accesului

- Conturi instituționale (nu personale) pentru activitatea didactică, cu 2FA obligatoriu.
- Proces clar de acordare și, mai ales, de **retragere** a accesului când un angajat pleacă.
- Acces la date pe principiul „strictul necesar".

Pregătire pentru incidente

- Un plan simplu: cine ce face, pe cine anunță și în ce ordine, dacă apare un incident.
- Backup centralizat al datelor importante.
- Canale de raportare cunoscute de tot personalul: **cyberskill.ro → Raportează** (preventiv) și **pnrisc.dnsc.ro / 1911** (incidente).

> **Începe mic**
>
> Nu e nevoie de un proiect complex. Trei măsuri — 2FA obligatoriu, backup centralizat și o sesiune anuală de conștientizare — reduc dramatic riscul la nivel de școală.

13 Idei de activități de conștientizare cu elevii

Cadrul didactic este cel mai bun multiplicator de bune practici. Iată idei simple de activități prin care le predai elevilor igiena cibernetică — adaptabile la vârstă.

Teme și mini-lecții

- **Recunoaște momeala:** arată exemple de mesaje de phishing și cere elevilor să spună ce e suspect.
- **Parole puternice:** exercițiu de creare a unei „fraze de acces" memorabile.
- **Amprenta digitală:** ce informații despre noi sunt publice și cât de ușor se găsesc.
- **Deepfake și surse:** cum verificăm dacă o imagine sau un clip este real.
- **Hărțuirea online:** ce facem dacă noi sau un coleg suntem țința; unde cerem ajutor.

Exerciții practice

- Joc de rol: „atacatorul și ținta" — elevii identifică tehnica de manipulare.
- Concurs de „găsește indiciul fals" într-un e-mail proiectat pe ecran.
- Discuție: „ce postăm și ce NU postăm" despre noi și despre alții.

Sprijin de la CyberShield

Asociația CyberShield susține sesiuni și campanii de conștientizare direct în școli, licee și universități. Pentru materiale sau o sesiune cu specialiști, contactează-ne prin **cybershield.org**.

Reține despre fotografii

Dacă desfășori activități online sau publici rezultate, nu include date personale sau imagini cu elevi identificabili fără consimțământul părinților (vezi capitolul 10).

14 Raportarea: unde și cum

Raportarea are două scopuri diferite: **prevenția** (avertizezi comunitatea despre o amenințare) și **răspunsul la incident** (ceri ajutor după ce ai fost afectat). Folosești canale diferite pentru fiecare.

A. Prevenție — ai văzut ceva suspect

Un mesaj de phishing, un site fals care imită o instituție, o tentativă de fraudă, un cont care te impersonează. Chiar dacă nu ai pățit nimic, raportarea ajută la avertizarea altor cadre didactice și școli.

Raportează pe portalul de raportare al Asociației:

cyberskill.ro → secțiunea „Raportează"

Trimite cât mai multe detalii: capturi de ecran, adresa expeditorului, linkul suspect (fără să dai click pe el).

B. Incident cibernetic — ai fost afectat

Cont spart, dispozitiv infectat, date furate, bani pierduți printr-o fraudă online. Aici raportezi pentru a primi sprijin și pentru ca incidentul să fie analizat oficial.

Raportează la DNSC (Directoratul Național de Securitate Cibernetică):

pnrisc.dnsc.ro · telefon 1911

1911 este linia de suport și consiliere pentru gestionarea unui atac cibernetic.

Alte canale, în funcție de situație

Situație	Unde raportezi
Amenințare suspectă (preventiv)	**cyberskill.ro → Raportează**
Incident cibernetic (ai fost victimă)	**pnrisc.dnsc.ro** și **1911** (DNSC)
Infracțiune (fraudă, furt de bani, șantaj)	Depune plângere la cea mai apropiată secție de poliție
Cont fals / impersonare pe rețele sociale	Raportare în platformă + cyberskill.ro
Date ale elevilor expuse	Conducerea școlii + responsabilul cu protecția datelor (DPO)

Reține pe scurt

Suspect → cyberskill.ro/Raportează. Victimă → pnrisc.dnsc.ro + 1911. Infracțiune → plângere la cea mai apropiată secție de poliție.

15 Ce faci dacă ai fost victima unui atac

Panica este cel mai prost sfătuitor. Ai un plan clar și acționează în ordine. Primele minute contează cel mai mult.

Pașii imediați (în primele 30 de minute)

1. **Izolează.** Deconectează dispozitivul de la internet dacă suspectezi malware/ransomware.
2. **Schimbă parolele** de pe un alt dispozitiv sigur, începând cu e-mailul (cheia tuturor conturilor), apoi conturile importante.
3. **Activează autentificarea în doi pași** oriunde nu o aveai deja.
4. **Verifică** activitatea recentă a conturilor și deconectează sesiunile necunoscute.
5. **Anunță** conducerea școlii dacă sunt implicate date ale elevilor sau conturi instituționale.
6. **Avertizează-ți contactele** dacă ești impersonat, ca să nu cadă și ei victime.
7. **Raportează** incidentul la **pnrisc.dnsc.ro** și sună la **1911**.

Scenarii frecvente, pas cu pas

Ți-a fost spart contul de e-mail

De pe alt dispozitiv: schimbă parola → activează 2FA → verifică și șterge regulile de redirecționare/filtrele create de atacator → verifică „dispozitive conectate" și deconectează-le → anunță contactele care ar fi putut primi mesaje false → raportează la pnrisc.dnsc.ro / 1911.

Ți s-a clonat contul de Facebook

Raportează profilul fals în Facebook → anunță public prietenii să nu accepte cererea și să nu reacționeze la mesaje → verifică și întărește securitatea contului real (parolă nouă + 2FA) → roagă-ți prietenii și cunoștințele să raporteze și ei contul-clonă în platformă.

Ai dat click pe un link și ai introdus parola

Presupune că parola e compromisă: schimb-o imediat peste tot unde o foloseai → activează 2FA → monitorizează conturile pentru activitate ciudată → raportează la pnrisc.dnsc.ro / 1911.

Ai pierdut bani printr-o fraudă

Sună imediat banca pentru a bloca/contesta tranzacția → depune plângere la cea mai apropiată secție de poliție → păstrează toate dovezile (mesaje, capturi) → raportează la pnrisc.dnsc.ro / 1911.

16 Mituri frecvente despre securitatea online

Câteva convingeri răspândite care pun cadrele didactice în pericol — și de ce sunt greșite.

Mitul	Realitatea
„Nu sunt o persoană importantă, cine să mă atace?"	Atacurile sunt în mare parte automate și nedirecționate. Ești țintă tocmai pentru că ai acces la date și contacte.
„Am antivirus, deci sunt protejat."	Antivirusul ajută, dar nu oprește phishingul sau parolele slabe. Securitatea e un set de obiceiuri, nu un singur program.
„O parolă complicată e suficientă."	Dacă o refolosești sau e furată printr-o scurgere de date, complexitatea nu mai contează. De aceea e nevoie de parole unice + 2FA.
„Recunosc imediat un e-mail fals."	Mesajele moderne, generate cu AI, sunt foarte convingătoare. Oricine poate fi păcălit sub presiune de timp.
„2FA e complicat și mă încetinește."	Durează câteva secunde și este cea mai eficientă măsură împotriva preluării conturilor.
„Dacă raportez, oricum nu se întâmplă nimic."	Raportarea (la cyberskill.ro sau DNSC) ajută la avertizarea altora și la blocarea atacatorilor. Prevenția e colectivă.
„Datele elevilor nu interesează pe nimeni."	Datele minorilor sunt foarte valoroase și protejate legal; expunerea lor are consecințe reale pentru elevi și școală.

17 Liste de verificare (checklists)

Bifează. Aceste liste sunt gândite să fie tipărite și folosite efectiv — la început de an, la configurarea unui instrument sau în caz de incident.

17.1 Igiena cibernetică personală de bază

- [ ] Am parole unice pentru fiecare cont important.
- [ ] Folosesc un manager de parole.
- [ ] Am activat autentificarea în doi pași pe e-mail.
- [ ] Am activat autentificarea în doi pași pe Facebook și pe conturile Google/Microsoft.
- [ ] Sistemul de operare și aplicațiile se actualizează automat.
- [ ] Am backup pentru materialele didactice importante, în două locuri.
- [ ] Ecranul telefonului și al laptopului se blochează automat.
- [ ] Conturile personale sunt separate de cele profesionale.

17.2 Început de an școlar

- [ ] Mi-am schimbat parolele importante.
- [ ] Am verificat cine are acces la clasele și materialele mele.
- [ ] Am revizuit setările de confidențialitate ale rețelelor sociale.
- [ ] Am stabilit regulile grupurilor de comunicare cu părinții/elevii.
- [ ] Am verificat că am consimțământul părinților pentru fotografii/filmări.

17.3 Recunoaște un mesaj de phishing

- [ ] Adresa expeditorului este corectă (nu o imitație cu litere schimbate)?
- [ ] Mi se creează un sentiment artificial de urgență sau frică?
- [ ] Linkul corespunde textului (verificat cu mouse-ul, fără click)?
- [ ] Mi se cer parole, coduri sau bani?
- [ ] Există greșeli de limbă sau formulări ciudate?
- [ ] Dacă am dubii: nu dau click și raportez la cyberskill.ro → Raportează.

17.4 Classroom / Teams

- [ ] Folosesc contul instituțional, cu 2FA activ.
- [ ] Linkul/codul clasei nu este public.
- [ ] Aprobarea participanților / sala de așteptare este activată.
- [ ] Închid ferestrele cu date personale înainte de a partaja ecranul.
- [ ] Verific periodic lista de membri ai clasei.

17.5 Grup de WhatsApp cu părinți/elevi

- [ ] Grupul are reguli clare, comunicate la început.
- [ ] Pentru anunțuri folosesc un grup în care scrie doar adminul.
- [ ] Nu postez date personale ale elevilor sau fotografii fără acord.
- [ ] Verific identitatea pe alt canal înainte de a reacționa la mesaje „urgente".

17.6 Catalog electronic

- [ ] Parola catalogului este unică și puternică.
- [ ] Am activat 2FA, dacă platforma o oferă.
- [ ] Accesez catalogul doar de pe dispozitive de încredere.
- [ ] Mă deconectez complet pe calculatoarele partajate.
- [ ] Nu salvez parola în browserul unui calculator comun.

17.7 „Am fost victima unui atac" urgență

- [ ] Am izolat dispozitivul afectat.
- [ ] Am schimbat parolele de pe un dispozitiv sigur (întâi e-mailul).
- [ ] Am activat 2FA peste tot.
- [ ] Am deconectat sesiunile necunoscute.
- [ ] Am anunțat conducerea școlii (dacă sunt implicate date/instituție).
- [ ] Mi-am avertizat contactele (dacă sunt impersonat).
- [ ] Am raportat la DNSC: pnrisc.dnsc.ro și 1911.
- [ ] Dacă am pierdut bani: am anunțat banca și am depus plângere la cea mai apropiată secție de poliție.

18 Fișă de raportare a incidentului (de tipărit)

Completează această fișă când gestionezi un incident. Te ajută să nu uiți niciun pas și să ai datele pregătite când raportezi la DNSC sau la conducerea școlii.

Câmp	Completează
Data și ora descoperirii	
Ce s-a întâmplat (pe scurt)	
Conturi / dispozitive afectate	
Ce date ar fi putut fi expuse	
Pași făcuți (parole schimbate, 2FA, sesiuni închise)	
Persoane / instituții anunțate	

Raportat la

- [ ] cyberskill.ro → secțiunea „Raportează" (preventiv / amenințare)
- [ ] DNSC — pnrisc.dnsc.ro
- [ ] DNSC — telefon 1911
- [ ] Conducerea școlii / DPO
- [ ] Poliție — plângere la cea mai apropiată secție de poliție (infracțiune / pierdere de bani)
- [ ] Telefonul Copilului 116 111 / 119 (dacă este implicat un copil)

> **Sfat**
>
> Păstrează dovezile (capturi de ecran, mesaje, e-mailuri) atașate acestei fișe. Ele sunt esențiale pentru analiză și pentru o eventuală plângere.

19 Resurse și contacte utile

Salvează aceste contacte. Într-o situație de criză, vrei să le ai la îndemână, nu să le cauți.

Pe scurt: unde mergi și pentru ce

Raportezi ceva suspect → cyberskill.ro (secțiunea Raportează). · **Ai fost victimă** → pnrisc.dnsc.ro + 1911. · **Vrei informații / noutăți** → cybershield.org, dnsc.ro, sigurantaonline.ro.

Raportează ceva suspect

cyberskill.ro

Portalul de raportare al Asociației, secțiunea **„Raportează"**. Aici semnalezi preventiv site-uri false, mesaje de phishing, tentative de fraudă sau conturi care te impersonează. Trimite capturi de ecran și adresa/linkul suspect (fără să dai click pe el). Fiecare raportare ajută la avertizarea altor cadre didactice și a altor școli.

Asociația Educație în Securitate Cibernetică – CyberShield

cybershield.org

Site-ul oficial al asociației care a elaborat acest ghid. Aici găsești noutăți și resurse de securitate cibernetică, descarci gratuit versiunea actualizată a ghidului și poți solicita o sesiune sau o campanie de conștientizare direct în școala ta.

DNSC — Directoratul Național de Securitate Cibernetică

dnsc.ro

Site-ul oficial al autorității naționale în domeniu. Publică avertizări de securitate, ghiduri și campanii pentru public, precum și o listă publică de domenii periculoase (blacklist) pe care o poți verifica înainte de a accesa un site nesigur.

DNSC — raportare incident cibernetic

1911

Dacă ai fost victima unui incident (cont spart, dispozitiv infectat, fraudă online), raportează pe platforma **pnrisc.dnsc.ro** și sună la **1911**. Vei primi suport și consiliere pentru a limita pagubele și a-ți recupera conturile. Păstrează dovezile (capturi, mesaje).

Siguranță online — informații

sigurantaonline.ro

Platformă dedicată siguranței în mediul online. Oferă articole, sfaturi practice și materiale ușor de înțeles, utile atât pentru cadrele didactice, cât și pentru elevi și părinți — potrivite inclusiv pentru orele de consiliere și dirigenție.

Adu securitatea cibernetică în școala ta

Asociația Educație în Securitate Cibernetică – CyberShield susține campanii de conștientizare și sesiuni de „igienă în securitate cibernetică" direct în școli, licee și universități. Dacă vrei o astfel de sesiune pentru colegii sau elevii tăi, contactează-ne prin **cybershield.org**.

20 Glosar de termeni

Termenii pe care îi vei întâlni, explicați simplu.

Termen	Explicație
Phishing	Mesaj-momeală care imită o sursă de încredere pentru a-ți fura date sau bani.
Smishing	Phishing prin SMS.
Vishing	Phishing prin apel telefonic („voice phishing").
Quishing	Phishing prin cod QR fals.
Malware	Program dăunător (virus, troian etc.) care infectează un dispozitiv.
Ransomware	Tip de malware care îți criptează fișierele și cere bani pentru deblocare.
2FA / MFA	Autentificare în doi (sau mai mulți) pași: parolă + un al doilea cod.
Inginerie socială	Manipulare psihologică pentru a te determina să faci o greșeală de securitate.
Deepfake	Imagine, voce sau video fals, generat de inteligență artificială.
Manager de parole	Aplicație care generează și stochează parolele tale în siguranță.
Backup	Copie de rezervă a fișierelor, păstrată separat.
GDPR	Regulamentul european privind protecția datelor cu caracter personal.
DPO	Responsabilul cu protecția datelor dintr-o instituție.
Oversharing	Expunerea excesivă de informații personale online.
Suprafață de atac	Totalitatea punctelor prin care poți fi atacat (conturi, dispozitive, aplicații).
Spear phishing	Phishing direcționat pe o anumită persoană, folosind informații reale despre ea.
DNSC	Directoratul Național de Securitate Cibernetică — unde raportezi incidentele (1911, pnrisc.dnsc.ro).