

Cybersecurity a scuola: la guida completa

Regole, spiegazioni ed esempi pratici per proteggere dati, dispositivi e persone: pensata per essere letta e usata da docenti, genitori e alunni, con approfondimenti su phishing, cyberbullismo, adescamento online e intelligenza artificiale.

 **Docenti**

 **Genitori**

 **Alunni**

20

pagine di approfondimento

3

percorsi per pubblico

70+

regole e consigli pratici

A CURA DI

Cristina Galfo

Esperta di informatica e formazione digitale, docente e web developer con quasi 20 anni di esperienza tra scuola pubblica e academy. Fondatrice di **Lezia Hub**, piattaforma con risorse su intelligenza artificiale e didattica digitale, e del blog Coding Creativo.

Vuoi un corso di formazione sulla sicurezza digitale per la tua scuola?

Scrivi a info@lezia.it

Cosa trovi in questa guida

La guida è pensata per essere consultata anche a capitoli separati: ogni sezione è autonoma e puoi partire da quella più utile per te.

	Sezione	Pagina
01	Perché parlare di cybersecurity a scuola	3
02	Glossario essenziale: le parole della sicurezza digitale	4
03	Le basi tecniche per tutti: password, 2FA, backup, aggiornamenti	5
04	Riconoscere il phishing: esempi pratici	6
05	Navigare in modo sicuro: le regole del browser	7
06	Password nel browser: perché evitarle e cosa usare	8
07	Docenti — Parte 1: accesso, dati, dispositivi condivisi	9
08	Docenti — Parte 2: phishing, cyberbullismo, privacy in classe	10
09	Genitori — Parte 1: dialogo e parental control per età	11
10	Genitori — Parte 2: privacy social, sharenting, segnali d'allarme	12
11	Alunni — Scuola primaria: le prime regole	13
12	Alunni — Scuola secondaria: password, reputazione, fake news	14
13	Cyberbullismo: riconoscerlo e affrontarlo	15
14	Adescamento online (grooming): segnali e risposta	16
15	Intelligenza artificiale, deepfake e nuovi rischi	17
16	Cosa fare in caso di incidente: checklist per scenario	18
17	Contatti e risorse utili	19
18	Nota metodologica e colophon	20

Perché parlare di cybersecurity a scuola

Computer, tablet e smartphone sono ormai strumenti quotidiani per studiare, insegnare e comunicare in famiglia. Portano grandi opportunità — accesso a informazioni, didattica digitale, contatti facilitati tra scuola e famiglia — ma anche rischi concreti: password deboli, truffe online, contenuti inadatti, cyberbullismo, furto di dati personali, adescamento. La buona notizia è che gran parte di questi rischi si riduce con poche abitudini corrette, semplici da imparare e da ripetere nel tempo.

Un problema di tutti, non solo "tecnico"

La sicurezza informatica viene spesso immaginata come una questione per esperti di informatica. In realtà, la maggior parte degli incidenti reali (account rubati, truffe, episodi di cyberbullismo) nasce da comportamenti quotidiani: una password riusata ovunque, un link cliccato senza pensarci, un dato personale condiviso con leggerezza. Per questo la parte più efficace della cybersecurity è culturale ed educativa, non solo tecnica.

Tre pubblici, un solo obiettivo

Questa guida si rivolge a tre pubblici con ruoli diversi ma complementari:

Docenti

Proteggono dati e strumenti didattici, e sono un modello di comportamento digitale per gli alunni.

Genitori

Accompagnano i figli nell'uso di dispositivi e piattaforme, dialogando più che vietando.

Alunni

Imparano a riconoscere i rischi e a chiedere aiuto quando serve, senza sentirsi in colpa.

Come è organizzata questa guida

Dopo un glossario essenziale e una sezione di basi tecniche valide per chiunque, la guida propone due pagine di approfondimento per ciascun pubblico. Seguono capitoli dedicati a tre temi delicati e trasversali — phishing, cyberbullismo, adescamento online — un capitolo sui rischi emergenti legati all'intelligenza artificiale, una checklist operativa in caso di incidente e un elenco di contatti utili.

Come usarla in classe o in famiglia

Ogni sezione può essere letta singolarmente e usata come base per una discussione: in classe come spunto per un'ora di educazione civica digitale, in famiglia come punto di partenza per definire insieme qualche regola condivisa.

Glossario essenziale

Le parole che ricorrono più spesso quando si parla di sicurezza digitale, spiegate in modo semplice.

Malware **TECNICO**

Termine generico per indicare software dannoso (virus, spyware, ransomware) progettato per danneggiare un dispositivo o rubare dati.

Phishing **TRUFFA**

Email, messaggi o siti falsi che imitano un mittente affidabile (banca, scuola, corriere) per rubare password o dati personali.

Smishing / Vishing **TRUFFA**

Varianti del phishing via SMS (smishing) o telefonata (vishing), spesso con toni di urgenza per far abbassare la guardia.

Ransomware **TECNICO**

Malware che blocca o cifra i file di un dispositivo, chiedendo un riscatto per sbloccarli. Il backup regolare è la difesa principale.

Autenticazione a due fattori (2FA) **DIFESA**

Sistema che richiede, oltre alla password, un secondo elemento (codice temporaneo, app, impronta) per accedere a un account.

Cyberbullismo **RELAZIONI**

Atti di prevaricazione o molestia ripetuti nel tempo, realizzati tramite strumenti digitali, capaci di ferire, minacciare o isolare una persona.

Grooming (adescamento online) **RELAZIONI**

Insieme di tecniche con cui un adulto costruisce gradualmente fiducia con un minore online, spesso isolandolo, per poi sfruttarlo.

Sexting **RELAZIONI**

Invio o condivisione di immagini o messaggi a sfondo sessuale tramite dispositivi digitali; può esporre a diffusione non voluta o ricatti.

Sharenting **PRIVACY**

Abitudine di genitori (o adulti) di condividere online, spesso in modo frequente, foto e informazioni sui propri figli minorenni.

Deepfake **IA**

Immagine, audio o video generato o alterato con intelligenza artificiale per far sembrare reale qualcosa che non lo è.

Impronta digitale (digital footprint) **PRIVACY**

Tracce che una persona lascia online nel tempo (post, foto, commenti, ricerche): può essere più difficile da cancellare di quanto sembri.

VPN **TECNICO**

Strumento che crea una connessione cifrata tra dispositivo e internet, utile soprattutto su reti Wi-Fi pubbliche non protette.

Le basi tecniche: 6 abitudini che fanno la differenza

Valgono per docenti, genitori e alunni più grandi: sono il fondamento su cui si appoggiano tutte le altre regole della guida.

1 Password lunghe, uniche e gestite con un password manager

Almeno 12 caratteri, idealmente una frase facile da ricordare ma difficile da indovinare (es. "IlMioGatto*Ama7Pizze!"). Non riutilizzare mai la stessa password su più siti: se un servizio subisce una violazione, tutti gli altri account con la stessa password diventano vulnerabili. Un password manager genera e ricorda le password al posto tuo.

2 Autenticazione a due fattori (2FA) ovunque sia disponibile

Attivala su email, registro elettronico, social e servizi bancari: anche se la password viene rubata, senza il secondo codice l'accesso resta bloccato. Preferisci app di autenticazione o chiavi fisiche a SMS, quando possibile.

3 Aggiornamenti sempre attivi

Sistema operativo, browser e app: gli aggiornamenti correggono falle di sicurezza scoperte nel tempo. Attiva gli aggiornamenti automatici dove puoi, invece di rimandarli.

4 Backup regolari con la regola del "3-2-1"

Tre copie dei file importanti, su due supporti diversi (es. disco esterno e cloud), di cui una conservata altrove. In caso di virus, guasto o smarrimento del dispositivo, i dati restano al sicuro.

5 Wi-Fi domestico e reti pubbliche protette

Cambia la password predefinita del router, usa cifratura WPA2/WPA3 e rete ospiti separata per i dispositivi degli invitati. Su Wi-Fi pubbliche, evita di inserire password o dati sensibili, o usa una VPN.

6 Antivirus e buon senso, non solo tecnologia

Un antivirus aggiornato aiuta, ma la difesa più efficace resta non cliccare link o allegati sospetti e verificare sempre la fonte prima di scaricare qualcosa.

Un consiglio in più

Prova a fare un piccolo "controllo di sicurezza" una volta ogni pochi mesi: verifica quali app hanno accesso ai tuoi account social, controlla se ci sono aggiornamenti in sospeso e assicurati che il backup funzioni davvero, provando a recuperare un file.

Riconoscere il phishing: esempi pratici

Il phishing è la truffa digitale più comune. Ecco come riconoscerlo, con un esempio commentato.

Da: "Segreteria Scuola" <segreteria-avvisi23@mail-notifiche.info> **dominio sospetto**

Oggetto: **Azione richiesta: verifica account entro 24 ore** **urgenza artificiale**

Gentile utente, **saluto generico**

il suo accesso al registro elettronico risulta sospeso per verifiche di sicurezza. Clicchi sul link seguente ed inserisca le sue credenziali per riattivare l'account entro 24 ore, pena la cancellazione dei dati. **minaccia di conseguenze**

[Verifica il tuo account →](#) **link non verificabile**

In pochi secondi, questo messaggio mostra cinque segnali tipici del phishing: un indirizzo mittente che imita ma non coincide con quello ufficiale, un saluto generico invece del nome della persona, un'urgenza costruita ad arte, una minaccia di conseguenze negative e un link che non permette di verificare davvero dove porta.

Segnali da controllare sempre

- | | |
|--|---|
| ✓ Mittente e dominio coerenti con l'ente reale | ✗ Toni di urgenza o minaccia ("entro 24 ore") |
| ✓ Il messaggio si rivolge a te per nome | ✗ Errori grammaticali o di formattazione insoliti |
| ✓ Nessuna richiesta di dati sensibili via email/SMS | ✗ Richieste di password, codici OTP o pagamenti |
| ✓ Il link, passandoci sopra, punta al sito ufficiale | ✗ Allegati inattesi da mittenti sconosciuti |

Cosa fare se hai un dubbio

Non cliccare link né rispondere. Verifica contattando l'ente attraverso un canale ufficiale già noto (numero di telefono della scuola, sito istituzionale digitato a mano) e non attraverso i contatti presenti nel messaggio sospetto.

Navigare in modo sicuro: le regole del browser

Il browser è lo strumento che usiamo di più: alcune impostazioni e abitudini riducono molto i rischi, senza bisogno di competenze tecniche avanzate.

1 Controlla sempre HTTPS e il lucchetto nella barra degli indirizzi

Indicano che la connessione tra te e il sito è cifrata. Attenzione però: non garantiscono che il sito sia affidabile, solo che i dati in transito sono protetti. Un sito falso può comunque avere HTTPS.

2 Tieni il browser sempre aggiornato

Gli aggiornamenti correggono falle di sicurezza scoperte nel tempo e migliorano i filtri anti-phishing integrati. Attiva gli aggiornamenti automatici dove possibile.

3 Installa solo estensioni necessarie e controllane i permessi

Un'estensione poco affidabile può leggere tutto ciò che digiti o visiti. Prima di installarne una, verifica chi l'ha pubblicata, le recensioni e quali permessi richiede: se chiede più accesso di quanto sembri necessario, è un segnale d'allarme.

4 Blocca popup e download automatici

Nelle impostazioni del browser puoi impedire l'apertura automatica di finestre pubblicitarie e il download di file senza una tua conferma esplicita.

5 Limita cookie e tracciamento di terze parti

Riduce la quantità di dati raccolti sulla tua navigazione da siti diversi da quello che stai visitando. La maggior parte dei browser offre un'opzione dedicata nelle impostazioni privacy.

6 Diffida dei primi risultati "sponsorizzati" nei motori di ricerca

Alcune truffe comprano spazi pubblicitari per comparire in cima ai risultati, imitando siti ufficiali (banche, corrieri, assistenza clienti). Controlla sempre l'indirizzo esatto prima di cliccare.

Navigazione in incognito: cosa fa davvero (e cosa no)

La modalità in incognito evita che cronologia, cookie e password digitate restino salvati *su quel dispositivo*: è utile su un computer condiviso a scuola o in biblioteca.

Non ti rende invisibile: il gestore della rete, il datore di lavoro/la scuola (su rete istituzionale) e i siti visitati possono comunque vedere la tua attività. Non è uno strumento di anonimato, solo di igiene su dispositivi condivisi.

Per le famiglie: motori di ricerca e filtri pensati per i più piccoli

Per i bambini più piccoli esistono motori di ricerca e impostazioni "famiglia" che filtrano automaticamente i contenuti inadatti direttamente a livello di rete domestica o di browser. Non sono infallibili, ma riducono l'esposizione accidentale a contenuti non adatti all'età, specialmente se il minore naviga senza supervisione diretta.

Password nel browser: perché evitarle e cosa usare

Salvare le password quando il browser lo propone è comodo, ma su dispositivi condivisi o in caso di furto può trasformarsi in un rischio concreto.

Comodo, ma rischioso

Chi ha accesso fisico a un dispositivo sbloccato può, in pochi passaggi, aprire le impostazioni del browser e visualizzare in chiaro tutte le password lì salvate: capita spesso su PC di famiglia condivisi tra più persone, o su dispositivi scolastici usati da più alunni. Inoltre, i cosiddetti malware "infostealer" sono progettati proprio per cercare e rubare il database delle password salvate nei browser. Infine, se l'account del browser è sincronizzato tra più dispositivi senza una protezione forte (2FA), un solo accesso compromesso espone tutte le password salvate contemporaneamente.

Cosa usare al posto

- ✓ Un password manager dedicato, con database cifrato e protetto da una master password
- ✓ Una master password lunga e unica, che non usi da nessun'altra parte
- ✓ L'autenticazione a due fattori attiva sull'account del password manager stesso
- ✓ La funzione di generazione automatica di password complesse, diverse per ogni sito

Un password manager dedicato cifra i dati in modo più robusto rispetto al salvataggio integrato nel browser e, a differenza di quest'ultimo, è pensato specificamente per resistere a tentativi di accesso non autorizzato.

Regole per dispositivi condivisi (scuola, famiglia, biblioteca)

- ✓ Non selezionare mai "salva password" quando il browser lo propone
- ✓ Disattiva la compilazione automatica di dati di pagamento e indirizzi
- ✓ Fai sempre logout dagli account, non limitarti a chiudere la scheda
- ✓ Usa la navigazione in incognito quando disponibile
- ✓ Segui le eventuali policy dell'istituto su cancellazione dati a fine sessione

Se hai già password salvate nel browser

Vai nelle impostazioni del browser, nella sezione dedicata alle password, e controlla l'elenco di quelle memorizzate. Valuta di trasferirle in un password manager dedicato e, una volta fatto, elimina quelle salvate nel browser: in questo modo eviti di avere due copie non allineate e riduci la superficie di rischio.



Docenti: accesso, dati, dispositivi condivisi

Proteggere l'accesso agli strumenti digitali

1 Password personale e mai condivisa

Per registro elettronico, posta istituzionale e piattaforme didattiche. Non prestarla a colleghi, collaboratori o supplenti: ognuno deve avere il proprio accesso.

2 Attiva la 2FA dove disponibile

Molte piattaforme scolastiche la offrono: protegge l'account anche se la password viene intercettata.

3 Fai sempre logout dai dispositivi condivisi

LIM, PC di laboratorio o tablet della classe: chiudi sempre la sessione a fine lezione o quando il dispositivo passa ad altri, anche per pochi minuti.

Gestire i dati degli studenti con cura

Voti, note disciplinari, documenti relativi a bisogni educativi speciali o situazioni familiari: sono dati particolarmente delicati. Vanno trattati seguendo le indicazioni della scuola e la normativa sulla protezione dei dati (GDPR), che per i minori prevede un livello di attenzione ancora più alto.

- ✓ Condividi questi dati solo con chi ha titolo per riceverli
- ✓ Non inviarli tramite chat o email personali non istituzionali
- ✓ Evita di lasciare documenti cartacei o digitali accessibili a terzi
- ✓ In caso di dubbio, chiedi indicazioni al referente privacy dell'istituto

Strumenti didattici: solo quelli approvati

App e siti non verificati dalla scuola possono raccogliere dati degli alunni in modo non conforme alla normativa sulla privacy dei minori, o esporli a pubblicità e contenuti inadatti. Prima di introdurre un nuovo strumento in classe, verifica che sia stato validato dall'istituto o dal referente per la trasformazione digitale.



Docenti: phishing, cyberbullismo, privacy in classe

Riconoscere il phishing rivolto alle scuole

Le scuole sono un bersaglio frequente: finte comunicazioni da "ministero", "segreteria" o "fornitori di materiale didattico" che chiedono credenziali, dati o pagamenti urgenti. Verifica sempre mittente e canale ufficiale prima di agire (vedi la sezione dedicata al phishing a pag. 6).

Il ruolo del docente nel cyberbullismo

Se un alunno segnala, direttamente o indirettamente, episodi di cyberbullismo, il modo in cui il docente reagisce nei primi minuti è decisivo.

- ✓ Ascolta senza giudicare e senza minimizzare quanto riferito
- ✓ Rassicura l'alunno: chiedere aiuto è sempre la scelta giusta
- ✓ Coinvolgi subito il referente scolastico per il cyberbullismo
- ✓ Informa la famiglia seguendo il protocollo dell'istituto
- ✓ Non chiedere all'alunno di "confrontarsi" da solo con chi lo ha offeso

Privacy durante attività digitali e didattica a distanza

Registrazioni di videolezioni, foto di attività in classe, condivisione di materiali con volti di minori: vanno gestite con il consenso previsto dalla scuola e conservate solo per il tempo necessario, su piattaforme approvate e non su dispositivi o cloud personali.

Essere un modello di comportamento digitale

Gli alunni imparano anche osservando: il modo in cui un docente gestisce notifiche, tempo online, toni nelle comunicazioni digitali con classe e famiglie è, di fatto, una lezione di educazione digitale continua.

Formazione continua

La sicurezza digitale evolve rapidamente: partecipare a percorsi di aggiornamento, anche brevi, aiuta a riconoscere nuove minacce (come quelle legate all'intelligenza artificiale, vedi pag. 17) prima che diventino un problema in classe.



Genitori: dialogo e parental control per età

Il dialogo prima del controllo

Un dialogo regolare, curioso e senza giudizio su cosa fanno i figli online è più efficace, nel tempo, del solo controllo tecnico. Chiedere "cosa stai giocando?" o "chi ti scrive più spesso?" con genuino interesse costruisce fiducia e rende più probabile che un figlio racconti un problema, invece di nascondere per paura di essere puniti o privati del dispositivo.

Parental control per fascia d'età

6-8 anni

Uso supervisionato e in spazi comuni della casa. Profili bambino con contenuti filtrati, nessun accesso autonomo a social o chat con sconosciuti, tempo schermo concordato insieme.

9-11 anni

Maggiore autonomia ma con filtri contenuti attivi e limiti di tempo. Prime spiegazioni su password personali e sul non condividere dati con sconosciuti online.

12-14 anni

Primi social e chat di gruppo: profili privati, restrizioni su acquisti in-app, dialogo su cyberbullismo e reputazione digitale. Riduzione graduale dei filtri automatici a favore della fiducia costruita insieme.

15-18 anni

Autonomia quasi completa: il controllo tecnico lascia spazio a un dialogo su privacy, sexting, fake news e gestione del tempo online, restando un punto di riferimento disponibile in caso di problemi.

Un promemoria utile

Nessun filtro sostituisce il dialogo: uno strumento tecnico può essere aggirato, una relazione di fiducia resta la protezione più solida nel tempo.



Genitori: privacy, sharenting, segnali d'allarme

Impostazioni privacy di social e app

Controlla insieme ai figli le impostazioni privacy degli account che usano: profilo privato invece che pubblico, posizione geografica disattivata, possibilità di essere contattati limitata ai soli contatti conosciuti. Rivedi queste impostazioni periodicamente: gli aggiornamenti delle app a volte le reimpostano ai valori predefiniti.

Attenzione allo "sharenting"

Foto, nome della scuola, orari e abitudini quotidiane dei figli pubblicati online, anche da parte dei genitori, possono esporre i minori a rischi non immediatamente evidenti. Prima di condividere un contenuto che li riguarda, chiediti chi potrà vederlo, per quanto tempo resterà online e se un giorno tuo figlio sarebbe d'accordo che fosse pubblico.

Riconoscere i segnali di disagio online

Alcuni comportamenti possono segnalare che qualcosa non va, senza che il figlio ne parli apertamente:

- ✓ Isolamento improvviso o cambi d'umore dopo l'uso del telefono
- ✓ Segretezza eccessiva su messaggi, contatti o attività online
- ✓ Nuovi contatti sconosciuti, spesso più grandi d'età
- ✓ Rifiuto improvviso di andare a scuola o di frequentare amici
- ✓ Regali, ricariche telefoniche o denaro di provenienza non chiara

Nessuno di questi segnali, da solo, è una prova certa: sono spunti per approfondire con calma, senza accusare.

Gaming, chat vocali e acquisti in-app

I videogiochi online spesso includono chat vocali o testuali con sconosciuti e acquisti in-app. Imposta limiti di spesa o richiedi conferma per gli acquisti, e valuta insieme quali giochi prevedono interazioni con estranei.



Alunni — Scuola primaria: le prime regole

Regole semplici, pensate per essere lette insieme a un adulto e ripetute spesso.

1 Usa il tablet o il computer solo con un adulto vicino

Soprattutto quando navighi, guardi video o giochi online.

2 Non dire mai la tua password, nemmeno a un amico

La password è come la chiave di casa: si tiene solo per sé.

3 Non scrivere il tuo nome, la scuola o l'indirizzo a chi non conosci

Se qualcuno che non conosci ti chiede queste cose, chiedi subito a un adulto cosa fare.

4 Se vedi qualcosa che ti spaventa o non capisci, chiudi e chiama un adulto

Non c'è nulla di sbagliato nel chiedere aiuto: è sempre la cosa giusta da fare.

5 Non premere mai "sì" o "accetto" senza chiedere

Prima di scaricare un gioco o accettare un messaggio, chiedi a un adulto.

Un gioco da fare insieme

Prova a chiedere al tuo bambino/a di raccontarti cosa fa online come se te lo stesse spiegando per la prima volta: aiuta a capire davvero cosa vede e con chi interagisce, e rende naturale parlarne anche in futuro.

**Password e dati personali****1 Non dare mai la tua password a nessuno**

Nemmeno a un amico o a chi dice di essere un "tecnico" o un "amministratore" di una piattaforma.

2 Non condividere dati personali con sconosciuti

Nome completo, scuola, indirizzo, numero di telefono: non si danno a chi si conosce solo online, anche se sembra simpatico.

Reputazione digitale

Una foto o un messaggio, una volta inviati, possono essere salvati e diffusi anche fuori dal tuo controllo. Prima di pubblicare o inviare qualcosa, chiediti se andrebbe bene fosse visto da un insegnante, dai tuoi genitori o da uno sconosciuto tra qualche anno.

Notizie e informazioni: verificare prima di credere

Non tutto ciò che è online è vero, nemmeno quando sembra ben fatto o condiviso da molte persone. Prima di credere o condividere una notizia, controlla se è riportata anche da fonti ufficiali o testate riconosciute.

Se qualcuno ti infastidisce online

- ✓ Non rispondere a provocazioni o insulti
- ✓ Salva screenshot come prova, senza cancellare nulla
- ✓ Blocca e segnala il profilo sulla piattaforma
- ✓ Parlane con un genitore, un insegnante o un adulto di fiducia

Ricorda

Internet è uno spazio reale: le regole di rispetto e buon senso che usi di persona valgono anche online. Se hai un dubbio, è sempre giusto chiedere a un adulto prima di agire — non sei tu ad aver sbagliato se qualcosa va storto.

Cyberbullismo: riconoscerlo e affrontarlo

Un fenomeno diverso dal bullismo tradizionale per alcune caratteristiche importanti da conoscere.

Cosa lo rende diverso

Continuità

Può proseguire 24 ore su 24, anche fuori dagli spazi e dagli orari scolastici.

Ampiezza

Un contenuto può raggiungere e essere visto da un numero molto ampio di persone.

Persistenza

Screenshot e condivisioni rendono difficile far sparire davvero un contenuto.

Se sei tu a subirlo

- ✓ Non rispondere e non cancellare i messaggi: sono una prova utile
- ✓ Blocca il profilo o il contatto responsabile
- ✓ Parlane con un adulto di fiducia il prima possibile
- ✓ Segnala il contenuto alla piattaforma e, se serve, alla scuola

Se sei testimone

Chi assiste senza intervenire, anche solo restando in silenzio in una chat di gruppo, contribuisce involontariamente a far proseguire l'episodio. Segnalare quanto visto a un adulto, anche senza esporsi pubblicamente, è un aiuto concreto per chi lo sta subendo.

Il quadro normativo in Italia

La Legge 71/2017 disciplina la prevenzione e il contrasto del cyberbullismo, prevede la figura del referente scolastico per il fenomeno e introduce, per la vittima o per i genitori di un minore di 14 anni, la possibilità di chiedere alla piattaforma la rimozione o l'oscuramento di un contenuto lesivo. Questa guida offre un'informazione generale e non sostituisce una consulenza legale: per situazioni specifiche è opportuno rivolgersi alla scuola o alle autorità competenti.

Adescamento online (grooming): segnali e risposta

Un tema delicato, importante da conoscere sia per genitori e docenti sia, con un linguaggio adeguato, per i ragazzi più grandi.

Come si sviluppa, in genere

Il grooming è un processo graduale: un adulto costruisce fiducia con un minore fingendo interesse, comprensione o affetto, spesso online, per poi isolarlo progressivamente da amici e famiglia e arrivare a richieste inappropriate. Non avviene sempre allo stesso modo, ma segue spesso una logica di avvicinamento lento e di costruzione di un legame esclusivo e segreto.

Segnali da non sottovalutare

- ✗ Un contatto online che chiede di "tenere il segreto" con i genitori
- ✗ Regali, ricariche o attenzioni particolari da un contatto adulto
- ✗ Insistenza nel voler passare dalla chat pubblica a canali privati
- ✗ Richieste di foto o informazioni personali progressivamente più intime
- ✗ Pressione emotiva o senso di colpa in caso di rifiuto

Cosa dire a un ragazzo o una ragazza

Un adulto che chiede di tenere segreti dai genitori, che fa regali senza motivo o che insiste per passare a conversazioni private non sta comportandosi in modo normale, anche se sembra gentile o comprensivo. Va sempre bene interrompere la conversazione e parlarne con un adulto di fiducia, senza sentirsi in colpa o temere di essere puniti.

Cosa fare come genitore o docente

Ascolta senza giudicare, non colpevolizzare mai il minore, conserva screenshot e messaggi come prova e rivolgiti alla Polizia Postale. In situazioni di questo tipo, agire con tempestività è più importante che avere ogni dettaglio chiaro fin da subito.

Intelligenza artificiale, deepfake e nuovi rischi

Strumenti di IA generativa sono ormai accessibili a chiunque: portano opportunità didattiche, ma anche rischi da conoscere.

Deepfake: quando non ci si può fidare degli occhi

Immagini, audio e video generati o alterati con l'IA possono far sembrare reale qualcosa che non lo è: un volto sovrapposto a un video, una voce clonata, un'immagine mai scattata. Sono già stati usati per creare contenuti diffamatori o falsi allarmi. Un contenuto sorprendente o allarmante andrebbe sempre verificato prima di essere creduto o condiviso.

Chatbot e assistenti IA: cosa condividere e cosa no

- ✓ Non inserire dati personali sensibili (indirizzi, documenti, password) nelle conversazioni con un chatbot
- ✓ Ricorda che le risposte possono contenere errori: verifica le informazioni importanti su fonti affidabili
- ✓ Usa questi strumenti come supporto allo studio, non come sostituto della verifica personale

Disinformazione generata dall'IA

Testi, immagini e video generati dall'IA rendono più facile produrre contenuti falsi ma credibili su larga scala. Le stesse regole di verifica delle fonti viste per le fake news (pag. 14) restano la difesa principale: controllare l'origine, cercare conferme su fonti ufficiali, diffidare di contenuti costruiti per suscitare una reazione emotiva immediata.

Per i docenti: un'opportunità educativa

Mostrare in classe esempi di deepfake o testi generati dall'IA, in modo consapevole, può essere un ottimo punto di partenza per allenare il pensiero critico digitale, più efficace di un semplice divieto d'uso.

Cosa fare in caso di incidente: checklist per scenario

Ogni situazione ha priorità leggermente diverse: ecco una guida rapida divisa per caso.

Account compromesso (password rubata)

- ✓ Cambia subito la password, da un dispositivo sicuro
- ✓ Attiva la 2FA se non era già attiva
- ✓ Controlla e revoca sessioni o dispositivi sconosciuti collegati
- ✓ Avvisa i tuoi contatti se l'account ha inviato messaggi sospetti

Truffa economica online

- ✓ Contatta subito la tua banca per bloccare la carta o il pagamento
- ✓ Conserva ricevute, messaggi e schermate della truffa
- ✓ Sporgi denuncia alla Polizia Postale

Cyberbullismo

- ✓ Non cancellare nulla: screenshot e messaggi sono prove utili
- ✓ Blocca il contatto e segnala il contenuto alla piattaforma
- ✓ Coinvolgi la scuola e il referente per il cyberbullismo
- ✓ Valuta, per i casi più gravi, la richiesta di oscuramento del contenuto

Adescamento o richieste inappropriate

- ✓ Interrompi la conversazione senza cancellare i messaggi
- ✓ Avvisa subito un adulto di fiducia
- ✓ Contatta la Polizia Postale

Dispositivo con virus o comportamento anomalo

- ✓ Disconnetti il dispositivo da internet
- ✓ Esegui una scansione con un antivirus aggiornato
- ✓ Cambia le password usate su quel dispositivo, da un altro dispositivo sicuro
- ✓ Ripristina da un backup pulito se il problema persiste

"Segnalare presto un problema è quasi sempre più semplice ed efficace che provare a risolverlo da soli in silenzio."

Contatti e risorse utili

Numeri e portali ufficiali di riferimento in Italia.

Polizia Postale — segnalazioni online	commissariatodips.it
Numero di pubblica utilità per l'infanzia	114 — Emergenza Infanzia
Linea di ascolto per bambini e adolescenti	19696 — Telefono Azzurro
Portale nazionale su educazione digitale e cyberbullismo	generazioniconnesse.it
Garante per la protezione dei dati personali	garanteprivacy.it
Ministero dell'Istruzione — area cyberbullismo	miur.gov.it

Per approfondire in classe o in famiglia

Molti portali istituzionali offrono materiali gratuiti (video, schede, percorsi) pensati per età diverse: possono essere un ottimo complemento a questa guida per un percorso più strutturato di educazione digitale.

Un'ultima cosa

Nessuna guida sostituisce l'attenzione quotidiana e il dialogo. Le regole aiutano, ma è la relazione tra adulti e ragazzi — a scuola e in famiglia — a fare davvero la differenza quando qualcosa va storto.

Nota metodologica e colophon

Questa guida raccoglie indicazioni di carattere generale sulla sicurezza digitale, rivolte a docenti, genitori e alunni. Non sostituisce una consulenza legale, tecnica o psicologica specialistica: per situazioni specifiche si raccomanda di rivolgersi alla scuola, alle autorità competenti o a professionisti qualificati.

Versione e licenza

Versione 2.0 — Edizione approfondita. Materiale didattico ad uso libero: può essere stampato, distribuito e adattato in contesti scolastici e familiari, citando la fonte.

Porta questo percorso nella tua scuola

Questa guida è pensata anche come base per un corso di formazione in presenza o online sulla sicurezza digitale, rivolto a colleghi docenti, consigli di istituto o gruppi di genitori.

Per richiedere informazioni: info@lezia.it

A cura di

Cristina Galfo — esperta di informatica e formazione digitale, docente e web developer con quasi 20 anni di esperienza tra scuola pubblica e academy. Fondatrice di **Lezia Hub**, piattaforma con risorse su intelligenza artificiale e didattica digitale, e del blog Coding Creativo.

Per corsi di formazione sulla sicurezza digitale: info@lezia.it

Nota: per generare questi contenuti si sono utilizzati, in alcuni punti, strumenti di intelligenza artificiale. Prima della distribuzione si consiglia una verifica da parte della scuola o di un referente competente, anche per adattare i contenuti al proprio contesto specifico e alla normativa vigente al momento della lettura.