

GIUGNO 2026

NUMERO 6

AttentiOnline Junior



Rivista di sicurezza online per elementari e medie

Cari ragazzi, genitori e insegnanti,

Siamo felicissimi di presentarvi **Attentionline Junior**, la nuova sezione del nostro sito pensata appositamente per i giovani esploratori del web delle scuole elementari e medie!

Internet è come un grande parco giochi pieno di opportunità: puoi imparare cose nuove, divertirti con i giochi, chattare con gli amici e scoprire mondi fantastici. Ma proprio come in un parco reale, anche online è importante conoscere le regole di sicurezza per evitare piccoli e grandi pericoli.

Cosa troverai su Attentionline Junior?

Abbiamo creato uno spazio colorato e divertente dove imparare a navigare in sicurezza diventa un gioco! Troverai:

- **Rebus e giochi "trova le differenze"** con immagini sulla sicurezza online: perché imparare divertendosi è il modo migliore per ricordare!
- **Guide semplici e chiare** per creare password sicure che proteggano i tuoi account come un vero scudo.
- **Un glossario speciale** con tutte le parole della sicurezza spiegate in modo semplice.
- **Fumetti e storie** con protagonisti che affrontano le stesse situazioni che potresti incontrare tu.
- **Video tutorial** creati appositamente per la tua età.

Perché Attentionline Junior?

Abbiamo notato che sempre più giovani navigano in internet a età sempre più precoci. Smartphone, tablet e computer sono strumenti fantastici, ma è importante imparare a usarli in modo sicuro fin da subito. Il nostro obiettivo è rendere i ragazzi consapevoli e preparati, trasformandoli in veri "supereroi digitali"! E ricorda: non sei mai troppo piccolo per essere attento e responsabile online!

Per genitori e insegnanti

Una sezione speciale sarà dedicata a voi adulti, con consigli pratici su come accompagnare i ragazzi nel mondo digitale, suggerimenti per il parental control e materiale didattico da utilizzare in classe o a casa.

Unisciti a noi in questa fantastica avventura digitale. **Attentionline Junior** è il posto dove la sicurezza online diventa un gioco da ragazzi!



"IL CODICE SEGRETO"

Matteo ha dieci anni e un problema urgente: vuole mandare un messaggio alla sua amica Elisa per organizzarle una festa di compleanno a sorpresa, ma il fratello maggiore Leonardo controlla sempre il telefono di casa e leggerebbe tutto. "Potremmo scrivervi in codice", gli dice Elisa un pomeriggio a scuola. "Ma come si fa?", chiede Matteo. "Non lo so", risponde lei. "Però una volta ho letto che lo faceva Giulio Cesare."

Quella sera Matteo chiede alla mamma, che è un'ingegnere informatico, se è vero che Giulio Cesare scriveva messaggi segreti. La mamma sorride. "Non solo è vero", gli dice, "ma il suo sistema era talmente geniale nella sua semplicità che lo studiamo ancora oggi, duemila anni dopo. E ogni volta che mandi un messaggio su WhatsApp, stai usando un suo pronipote lontanissimo."

Il sistema di Cesare funzionava così: quando doveva mandare un ordine segreto ai suoi generali, prendeva ogni lettera del messaggio e la sostituiva con quella che nell'alfabeto si trova tre posizioni più avanti. La A diventava D, la B diventava E, la C diventava F, e così via. Se doveva scrivere "ATTACCO ALL'ALBA", il messaggio diventava un insieme di lettere senza senso per chiunque lo intercettasse. Ma il generale che lo riceveva sapeva che bastava spostare ogni lettera di tre posizioni all'indietro per leggere il messaggio originale. Quel numero tre era la "chiave": il segreto condiviso tra chi scriveva e chi leggeva.

Al tempo di Cesare il sistema era sicuro per una ragione che oggi ci sembra incredibile: la maggior parte dei nemici non sapeva nemmeno leggere, figuriamoci decifrare un codice. Ma il cifrario di Cesare ha un difetto enorme: le chiavi possibili sono pochissime. Nell'alfabeto ci sono 26 lettere, quindi le chiavi possibili sono solo 25 (non 26, perché la chiave zero lascerebbe il messaggio identico). Questo significa che un nemico paziente potrebbe provare tutte e 25 le possibilità e trovare quella giusta in pochi minuti. Non a caso, quando Maria Stuarda, la regina di Scozia, provò a usare un sistema simile per organizzare un complotto contro la regina Elisabetta I d'Inghilterra nel 1586, il messaggio fu decifrato quasi subito dalla spia di corte Francis Walsingham. E a Maria Stuarda quella leggerezza costò la testa. Letteralmente.

"Ma allora", chiede Matteo, "se il cifrario di Cesare è così facile da rompere, come si fa oggi a proteggere i messaggi?"

La mamma gli spiega che il principio è rimasto lo stesso: prendere un messaggio leggibile e trasformarlo in qualcosa di incomprensibile, usando una chiave che solo il mittente e il destinatario conoscono. Quello che è cambiato è la complessità. Il cifrario di Cesare ha 25 chiavi possibili. I sistemi che usiamo oggi ne hanno un numero così grande che ha più di 300 cifre. Per fare un confronto: anche se mettessimo tutti i computer del mondo a lavorare insieme per provare tutte le chiavi possibili, ci vorrebbero miliardi di



anni per trovare quella giusta.

La storia più famosa di messaggi segreti è quella della macchina Enigma, durante la Seconda guerra mondiale. L'ingegnere tedesco Arthur Scherbius aveva brevettato nel 1918 una macchina che sembrava una macchina da scrivere, ma faceva qualcosa di straordinario: ogni volta che premiavi un tasto, la lettera veniva sostituita con un'altra secondo uno schema che cambiava a ogni singola lettera. E ogni giorno i tedeschi cambiavano le impostazioni della macchina, rendendo il codice del giorno prima completamente inutile. I nazisti la usavano per cifrare tutti gli ordini militari, e per anni gli Alleati non riuscirono a capire cosa si dicessero.

Fu un matematico inglese di nome Alan Turing, insieme a un gruppo di colleghi riuniti in una base segreta chiamata Bletchley Park, a cambiare le cose. Turing ebbe un'intuizione geniale: una macchina poteva essere battuta solo da un'altra macchina. Costruì un dispositivo chiamato "Bombe" che riusciva a decifrare i codici tedeschi. Il suo lavoro, però, non partì da zero: si basava sulle ricerche dei matematici polacchi guidati da Marian Rejewski, che già nel 1932 erano riusciti a decifrare le prime versioni di Enigma. Secondo diversi storici, la decifrazione di Enigma contribuì ad accorciare la guerra di almeno due anni, salvando milioni di vite. E la cosa più bella è che Alan Turing è considerato oggi uno dei padri dell'informatica: le idee che usò per decifrare Enigma sono le stesse su cui si basano i computer che usiamo ogni giorno.

"E WhatsApp?", chiede Matteo. "WhatsApp come c'entra?"

C'entra eccome. Ogni volta che Matteo manda un messaggio a Elisa su WhatsApp, quel messaggio viene cifrato automaticamente dal suo telefono prima ancora di partire. Viaggia attraverso internet sotto forma di un codice incomprensibile, passa attraverso i server di WhatsApp (che non possono leggerlo, perché non hanno la chiave), e arriva sul telefono di Elisa, dove viene decifrato e torna leggibile. Questo sistema si chiama "crittografia end-to-end", che significa "da un capo all'altro": solo i due telefoni alle estremità della conversazione possono leggere il messaggio. Tutto quello che sta in mezzo, compresa WhatsApp stessa, vede solo un miscuglio di lettere e numeri senza senso.

È come se Matteo mettesse il suo messaggio in una scatola chiusa con un lucchetto speciale, di cui esistono solo due chiavi al mondo: una nel suo telefono e una in quello di Elisa. Il messaggio viaggia attraverso mille mani, ma nessuno può aprire la scatola. Solo Elisa, con la sua chiave.

Matteo quella sera prova il cifrario di Cesare con Elisa. Decidono di usare la stessa chiave di Giulio Cesare: 3. Il primo messaggio che Matteo cifra è "IHVWD D FDVD VDEDWR". Elisa ci mette un po', sposta ogni lettera di tre posizioni all'indietro, e scopre il messaggio: "FESTA A CASA SABATO". Ride. Poi gli scrive: "HYLYD". Matteo sposta le lettere e legge: "EVVIVA".

Leonardo, il fratello maggiore, trova il bigliettino. Lo guarda, non capisce niente, e lo butta via. Il codice segreto ha funzionato.

La mamma di Matteo, che ha visto tutta la scena, sorride. Duemila anni dopo Giulio Cesare, il principio è sempre lo stesso: un messaggio che solo chi ha la chiave giusta può leggere. Solo che oggi le chiavi non sono un numero da 1 a 25, ma numeri così grandi che nessun computer al mondo riuscirebbe a indovinarli. E tutto succede in automatico, ogni volta che premi "invio", senza che tu debba fare niente. La crittografia non è solo una cosa da spie e da generali romani. È qualcosa che ti protegge ogni giorno, in silenzio, ogni volta che scrivi a un amico.

Lo sapevi?

Lo storico romano Svetonio racconta che Giulio Cesare usava una chiave di 3 per cifrare la corrispondenza militare inviata ai suoi generali. Suo nipote Augusto usava lo stesso sistema, ma con una chiave di 1: la A diventava B, la B diventava C, e così via. Il cifrario di Cesare è considerato uno dei primi sistemi di crittografia della storia, anche se oggi sarebbe facilissimo da decifrare: basterebbe provare le 25 chiavi possibili una per una.

La macchina Enigma fu brevettata dall'ingegnere tedesco Arthur Scherbius nel 1918. Durante la Seconda guerra mondiale i nazisti la usarono per cifrare tutte le comunicazioni militari, cambiando le impostazioni ogni giorno. A Bletchley Park, in Inghilterra, il matematico Alan Turing e il suo gruppo costruirono una macchina chiamata "Bombe" che riuscì a decifrare i codici tedeschi, partendo dal lavoro dei matematici polacchi guidati da Marian Rejewski che già nel 1932 avevano violato le prime versioni di Enigma. Secondo diversi storici, la decifrazione di Enigma contribuì ad accorciare la guerra di almeno due anni.

WhatsApp utilizza la crittografia end-to-end su tutti i messaggi, le foto, i video e le chiamate dal 2016. Questo significa che nemmeno WhatsApp stessa può leggere i tuoi messaggi: solo il telefono di chi scrive e il telefono di chi riceve hanno le chiavi per decifrarli. Il sistema si basa sul protocollo Signal, lo stesso usato dall'app Signal, considerata una delle più sicure al mondo.

SPAZIO INSEGNANTI

Attività per la classe

DECIFRA I MESSAGGI SEGRETI

I ragazzi usano il cifrario di Cesare con chiavi diverse per decifrare messaggi legati alla sicurezza online. Sviluppa ragionamento logico, concentrazione e introduce il concetto di protezione dei dati attraverso la crittografia.

CHIAVE = 3

A	B	C	D	E	F	G	H	I	...	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	...	A	B	C

MESSAGGIO CIFRATO: KRULVD QLQXQ SXD OHJJHUH

MESSAGGIO ORIGINALE: SICUREZZA ONLINE PER TUTTI

L'ENIGMA DEI NUMERI

Operazioni matematiche che permettono di scoprire una frase nascosta sulla sicurezza digitale. Unisce matematica, concentrazione e sicurezza online.

$$81 \div 3 = 27 \rightarrow A$$

$$(25 - 7) \times 2 = 36 \rightarrow L$$

$$144 \div 12 - 2 = 10 \rightarrow L$$

$$100 - 73 = 27 \rightarrow A$$

...

FRASE NASCOSTA: ALLA SICUREZZA PENSA PRIMA!

IDEE RAPIDE PER LA CLASSE

SFIDA "QUANTO TEMPO?"

Ogni alunno annota per una settimana il tempo trascorso su ciascuna app, poi la classe confronta i dati e discute le scoperte.

DIBATTITO GUIDATO

"Le app sono progettate per trattenerti: è giusto o sbagliato?". Dividere la classe in due squadre che argomentano posizioni opposte.

IL POSTINO SEGRETO

Per una giornata i messaggi tra compagni (bigliettini, note) devono essere cifrati con il cifrario di Cesare. Chi intercetta un messaggio e lo decifra guadagna un punto.

CHIAVE = 5

RJQH W XQ

DSW XQ L N G I J K O

CACCIA AL CODICE

L'insegnante nasconde in classe cinque messaggi cifrati con chiavi diverse. Ogni messaggio decifrato contiene un indizio per trovare il successivo.

INDIZIO SUCCESSIVO IN BIBLIOTECA!

Quella recensione è finta!

Lorenzo ha dodici anni e un problema: le sue cuffie si sono rotte. Ne vuole un paio nuove, possibilmente belle, con un buon suono, e che non costino una fortuna. Fa quello che fanno tutti: prende il telefono e cerca "migliori cuffie bluetooth economiche". I risultati sono tantissimi. Apre un sito e trova un paio di cuffie a 19 euro con 1.347 recensioni, media di 4,8 stelle su 5. "Qualità pazzesca!", scrive un utente. "Le migliori cuffie della mia vita!", scrive un altro. "Suono incredibile, sembrano cuffie da 200 euro!", aggiunge un terzo. Lorenzo è quasi convinto. Poi fa una cosa intelligente: fa vedere il sito a sua sorella maggiore, che studia informatica all'università.

La sorella guarda lo schermo per dieci secondi e dice: "Lorenzo, quelle recensioni sono false."

Lorenzo non capisce. Come possono essere false? Ci sono nomi, stelline, commenti. Qualcuno le ha scritte. "Certo che qualcuno le ha scritte", risponde la sorella. "Ma non qualcuno che ha comprato quelle cuffie. Qualcuno che è stato pagato per scrivere che sono fantastiche."

Questa è una delle cose che pochi ragazzi sanno, e che anche molti adulti ignorano: su internet esistono persone e perfino programmi automatici il cui unico lavoro è scrivere recensioni false. Vengono pagati per ogni recensione, oppure ricevono il prodotto gratis in cambio di cinque stelle. Esistono veri e propri operatori che vendono pacchetti di recensioni non autentiche, e nel giro di una notte un prodotto scadente si ritrova con una valutazione stellare. Funziona anche al contrario: a volte le recensioni negative sono scritte dai concorrenti per danneggiare un rivale. In Italia l'Autorità garante della concorrenza (AGCM) ha già sanzionato aziende per queste pratiche, considerate scorrette ai sensi del Codice del consumo, ma il fenomeno è talmente diffuso che è quasi impossibile fermarlo del tutto.

La sorella di Lorenzo gli insegna a riconoscere alcuni segnali che possono rivelare una recensione sospetta, e il metodo è più semplice di quanto sembri. La prima cosa da guardare è il profilo di chi ha scritto la recensione. Se clicchi sul nome del recensore e scopri che ha un account creato il giorno prima, senza foto, e che ha lasciato 47 recensioni entusiastiche a 47 prodotti diversi in una sola settimana, qualcosa non torna. Una persona vera compra un paio di cuffie, le prova, e dopo qualche giorno scrive cosa ne pensa. Non compra 47 prodotti in una settimana e non scrive 47 volte "prodotto fantastico, lo consiglio a tutti!".



La seconda cosa è il linguaggio. Le recensioni false si riconoscono spesso perché sono troppo generiche: "Ottimo prodotto!", "Molto soddisfatto!", "Lo ricomprirei subito!". Non dicono niente di specifico. Una persona che ha davvero usato quelle cuffie scriverebbe qualcosa come "il suono è buono ma i bassi sono un po' deboli" oppure "dopo due ore che le indosso cominciano a fare male alle orecchie". I dettagli concreti, i piccoli difetti, le osservazioni personali sono il segno che qualcuno ha davvero provato quel prodotto. Quando tutte le recensioni sembrano scritte dalla stessa persona e dicono tutte la stessa cosa, c'è da insospettirsi.

La terza cosa è la distribuzione delle stelle. Un prodotto vero ha recensioni di tutti i tipi: qualcuno lo ama, qualcuno lo odia, la maggior parte sta nel mezzo. Se un prodotto ha cinquecento recensioni e sono quasi tutte a cinque stelle, con pochissime a quattro e quasi nessuna a una, due o tre, è possibile che quelle a cinque stelle siano comprate. Nella vita reale nessun prodotto piace a tutti allo stesso modo.

La quarta cosa è controllare le date. Se un prodotto riceve trecento recensioni in tre giorni e poi più niente per mesi, probabilmente quelle trecento recensioni sono arrivate tutte insieme perché sono state acquistate in blocco. Le recensioni vere si accumulano gradualmente nel tempo, una ogni tanto, come succede quando le persone comprano il prodotto in momenti diversi e ci mettono qualche giorno a scrivere la loro opinione.

Nessuno di questi segnali, preso da solo, è una prova certa. Ma quando ne trovi due o tre insieme, è un buon motivo per diffidare e cercare altrove.

Ma le recensioni false non sono l'unico inganno in cui Lorenzo potrebbe cadere. Ci sono anche i negozi online completamente falsi. La sorella gli mostra un sito che vende scarpe di marca a prezzi incredibili: Nike Air Max a 29 euro, Adidas a 24 euro. Il sito è fatto bene, ha le foto dei prodotti, un carrello, una pagina di pagamento. Sembra un vero negozio. Ma ci sono dei segnali che lo tradiscono: l'indirizzo del sito è strano (qualcosa come "nike-supersconti-italia.xyz" invece di "nike.com"), non c'è una partita IVA visibile, non c'è un indirizzo fisico, non c'è un numero di telefono vero, e i prezzi sono troppo belli per essere veri. Questi siti esistono per un solo scopo: rubare i dati della carta di credito di chi prova a comprare qualcosa. Il pacco non arriverà mai, e nel frattempo qualcuno dall'altra parte del mondo ha il numero della carta dei tuoi genitori.

E poi c'è un terzo tipo di inganno, forse il più subdolo di tutti, perché non sembra nemmeno pubblicità: gli influencer che promuovono prodotti senza dire che sono pagati per farlo. Lorenzo segue su Instagram un ragazzo che fa video sui videogiochi. Un giorno questo ragazzo pubblica un video in cui dice "ragazzi, ho scoperto queste cuffie pazzesche, le uso da una settimana e il suono è incredibile, vi lascio il link". Lorenzo si fida: non è una pubblicità, è un consiglio di una persona che segue e che gli piace. Ma in realtà quel ragazzo ha ricevuto le cuffie gratis dall'azienda, o è stato pagato per parlarne bene. E non lo dice.

In Italia l'AGCOM ha adottato nel 2025 apposite linee guida sugli influencer, chiarite poi nel 2026 con FAQ operative. La regola principale è questa: quando un influencer pubblica un contenuto promozionale

IL DETECTIVE DEL WEB!

deve segnalarlo chiaramente con diciture come "Pubblicità", "ADV" o "Sponsorizzato da", e queste scritte devono essere visibili subito, senza che l'utente debba cliccare o scorrere per trovarle. Non bastano più espressioni vaghe come "in collaborazione con" perché non rendono chiaro che si tratta di pubblicità. Perfino quando un influencer riceve un prodotto gratuitamente senza essere pagato deve segnalarlo, per esempio con la dicitura "prodotto inviato da" o "gifted by". Chi non rispetta queste regole può andare incontro a diffide e sanzioni da parte dell'Autorità.

Il problema è che molti influencer ancora non lo fanno, o lo fanno in modo furbo: mettono la scritta "ADV" piccolissima, in un colore che si confonde con lo sfondo, oppure la nascondono tra decine di altri hashtag. Per questo è importante che anche i ragazzi sappiano riconoscere quando un "consiglio sincero" è in realtà una pubblicità. La regola è semplice: se qualcuno ti mostra un prodotto e ti dà un link per comprarlo o un codice sconto, quasi certamente guadagna qualcosa da quel link o da quel codice. Non significa che il prodotto sia per forza cattivo, ma significa che quel consiglio non è disinteressato come sembra.

Lorenzo alla fine non compra le cuffie da 19 euro con le recensioni sospette. Insieme alla sorella ne trova un paio da 35 euro con meno recensioni, ma tutte dettagliate, con pregi e difetti, scritte da persone che raccontano come le usano davvero. Costano un po' di più, ma quando arrivano funzionano esattamente come promesso. Ha imparato una lezione che vale per tutto quello che si compra, si legge e si guarda online: il fatto che qualcosa abbia tante stelline, tanti like o tanti commenti entusiasti non significa che sia vero. Significa solo che qualcuno ha voluto che sembrasse vero. E la differenza, con un po' di attenzione, si vede.

LO SAPEVI?

Nel mondo circa una recensione online su tre è falsa. Hai letto bene: su ogni tre recensioni che trovi su internet, una potrebbe essere stata scritta da qualcuno che non ha mai visto né toccato quel prodotto. L'industria delle recensioni false vale circa 15 miliardi di dollari a livello globale, ed esistono vere e proprie "fabbriche di recensioni": edifici pieni di lavoratori, spesso in paesi dove la manodopera costa poco, dove ogni persona gestisce decine di account falsi e scrive recensioni per prodotti diversi tutto il giorno, seguendo un copione. Un singolo aumento di una stella nella valutazione media di un prodotto su Amazon può far crescere le vendite dal 5 al 9 per cento: ecco perché per un venditore pagare 3-5 dollari per ogni recensione falsa è un investimento che rende moltissimo.

Solo nel 2024 Google ha bloccato o rimosso 240 milioni di recensioni che violavano le sue regole, e Amazon ha speso oltre 500 milioni di dollari in un solo anno e assunto 8.000 persone dedicate esclusivamente alla caccia alle recensioni false. Eppure il problema continua a crescere: il numero di recensioni false aumenta del 12 per cento più velocemente del numero di recensioni vere. Secondo una stima, nel 2025 le recensioni false hanno fatto spendere ai consumatori di tutto il mondo circa 770 miliardi di dollari in acquisti che non avrebbero fatto se le valutazioni fossero state oneste.

In questo numero trovi anche il poster "Sicuri online, sempre!", con i principali pericoli del web e le 7 regole d'oro per difenderti. Staccalo e appendilo in camera o in classe. In ogni prossimo numero di AttentiOnline Junior uscirà un nuovo poster dedicato a un pericolo specifico: collezionali tutti!

SICURI ONLINE, SEMPRE!

CONOSCI I PERICOLI. IMPARA A DIFENDERTI.



I PRINCIPALI PERICOLI DEL WEB

TRUFFE E IMBROGLI



Finti premi, regali o offerte incredibili possono nascondere truffe per rubare i tuoi dati o soldi.

INFORMAZIONI PERSONALI



Condividere troppi dati personali può metterti a rischio e far sapere a sconosciuti cose su di te.

CYBERBULLISMO



Insulti, minacce o esclusioni online fanno male quanto quelli di persona.
Non sei solo: parlane con un adulto.

CONTENUTI INAPPROPRIATI



Alcuni contenuti possono spaventare, turbare o essere inadatti alla tua età.
Se li trovi, chiudi e chiedi aiuto.

FALSI AMICI



Non tutti online sono quello che dicono.
Sconosciuti possono fingere di essere amici per ingannarti.

COME DIFENDERSI: LE 7 REGOLE D'ORO

1 PENSA PRIMA DI CLICCARE



Non cliccare su link sospetti o allegati di email sconosciute.

2 PROTEGGI I TUOI DATI PERSONALI



Non condividere mai nome, indirizzo, scuola, foto o numero di telefono.

3 USA PASSWORD SICURE



Crea password lunghe e difficili da indovinare. Non dirle a nessuno!

4 CHIEDI AIUTO A UN ADULTO



Se qualcosa ti mette a disagio, parlane subito con un genitore o un insegnante.

5 RISPETTA GLI ALTRI ONLINE



Sii gentile e rispetta gli altri. Le tue parole hanno valore, anche online.

6 IMPOSTA LA PRIVACY



Usa le impostazioni di privacy per decidere chi può vedere i tuoi contenuti.

7 FAI PAUSE E VIVI IL MONDO REALE



Troppo tempo online può farti male. Ricorda: ci sono tante cose belle anche fuori dallo schermo!

DOVE CHIEDERE AIUTO

PARLA SEMPRE CON QUALCUNO DI CUI TI FIDI.



GENITORI



INSEGNANTI



TELEFONO AZZURRO
19696
24 ORE SU 24



POLIZIA POSTALE
E DELLE
COMUNICAZIONI
poliziadistato.it

RICORDA:

- ✓ TU SEI IL PROTAGONISTA DELLA TUA SICUREZZA ONLINE!
- ✓ INTERNET È UNO STRUMENTO FANTASTICO: USALO CON INTELLIGENZA E RESPONSABILITÀ.
- ✓ SEI TU A DECIDERE COSA CONDIVIDERE E CON CHI.



LA TUA SICUREZZA ONLINE INIZIA DA TE. OGNI GIORNO!



TROVA I PERICOLI – "Aiuto, non riesco a smettere!"

Camilla ha undici anni e stasera ha deciso di andare a letto presto. Domani c'è la verifica di matematica e vuole essere riposata. Si lava i denti, si mette il pigiama, si infila sotto le coperte. Poi prende il telefono dal comodino. Solo per un secondo, si dice. Vuole guardare un video che le ha mandato un'amica su TikTok: un gatto che gioca con una scatola di cartone. Dura venti secondi, è buffo. Camilla sorride.

Ma il video finisce e ne parte subito un altro. Un ragazzo che cucina una torta a forma di dinosauro. Non le interessa particolarmente, ma è già iniziato, quindi lo guarda fino alla fine. Poi ne arriva un altro: una ragazza che mostra come disegnare un drago in trenta secondi. Bello! E poi un altro. E un altro. E un altro ancora.

Quando Camilla alza lo sguardo dallo schermo e guarda l'orologio, sono le 23:37. Sono passate quasi due ore. Due ore in cui voleva guardare un solo video di venti secondi.

Camilla non ha fatto niente di sbagliato, non è pigra, non è "malata di telefono". È una ragazzina normale che è finita dentro un meccanismo progettato apposta per fare esattamente quello che è successo: impedirti di smettere. E per capire come funziona questo meccanismo bisogna sapere una cosa: le app come TikTok, YouTube e Instagram non funzionano come un libro o un film. Un libro ha un'ultima pagina. Un film ha i titoli di coda. A un certo punto finiscono, e tu smetti naturalmente di guardarli perché non c'è più niente da guardare. È come un piatto di pasta: finisci quello che c'è nel piatto e ti fermi.

Le app di video e i social, invece, non finiscono mai. Non c'è un'ultima pagina, non ci sono titoli di coda, non c'è un fondo del piatto. Puoi scorrere in basso con il dito per ore e ci saranno sempre nuovi contenuti, uno dopo l'altro, senza interruzione. Questa funzione si chiama "scroll infinito" ed è stata progettata apposta per tenerti dentro l'app il più a lungo possibile. Il motivo è semplice: più tempo passi dentro l'app, più pubblicità puoi vedere, e più soldi guadagna chi l'ha creata. Tu non paghi per usare TikTok o Instagram, ma le aziende pagano per mostrarti la pubblicità mentre li usi, e pagano di più se tu resti lì a lungo. Per questo ogni dettaglio dell'app è costruito per farti restare: i video che partono da soli senza chiederti niente, le notifiche che ti richiamano quando esci, i contenuti che sembrano sempre esattamente quelli che piacciono a te.

C'è un motivo per cui è così difficile fermarsi, e non c'entra la forza di volontà. C'entra il modo in cui funziona il nostro cervello. Dentro il cervello esiste una sostanza che si chiama dopamina. Non è una droga e non è pericolosa: è una sostanza naturale che il cervello produce quando succede qualcosa di piacevole o di nuovo. Quando mangi qualcosa di buono, il cervello produce un po' di dopamina. Quando un amico ti fa ridere, un po' di dopamina. Quando apri un regalo e scopri cosa c'è dentro, un po' di dopamina. Il punto è che il cervello ama la novità, e ogni nuovo video è una piccola novità. Non sai mai cosa apparirà dopo, e questa incertezza è esattamente il tipo di situazione che fa produrre dopamina e che spinge a voler vedere il prossimo video. È come avere una scatola infinita di cioccolatini, ognuno con un gusto diverso: ne prendi uno, lo assaggi, e il cervello dice "chissà com'è il prossimo!". E allora ne prendi un altro, e poi un altro, e poi un altro.

Le app lo sanno. Lo sanno benissimo. E usano questa conoscenza per progettare l'esperienza nel modo più coinvolgente possibile. Non è un caso che i video partano da soli senza chiederti niente: quel mezzo secondo in cui dovresti decidere se guardare il prossimo video o chiudere l'app sarebbe il momento in cui potresti fermarti. Eliminando quel momento, la scelta viene fatta al posto tuo. E c'è una cosa che rende tutto ancora più efficace: l'algoritmo. Ogni volta che guardi un video fino alla fine, l'app prende nota. Se guardi tre video di cucina di fila, l'app prende nota. Piano piano, senza che tu te ne accorga, l'app costruisce un tuo ritratto mol-



to preciso: sa cosa ti piace, cosa ti annoia, a che ora del giorno sei più attiva, quanto tempo tendi a restare. Ed ecco la cosa più importante di tutto questo articolo, e vale la pena ripeterla: se ti è capitato di perdere il senso del tempo guardando video, non è perché sei debole o hai fatto qualcosa di sbagliato. È perché dall'altra parte dello schermo ci sono centinaia di ingegneri, psicologi e matematici il cui lavoro è esattamente quello: rendere quell'app così coinvolgente che tu non riesca a smettere. Uno di questi ingegneri si chiama Aza Raskin. Nel 2006 ha contribuito a rendere popolare lo scroll infinito. Anni dopo, ha dichiarato pubblicamente di essersi pentito, perché si è reso conto di quanto tempo la sua invenzione fa perdere alle persone ogni giorno. Oggi è cofondatore del Center for Humane Technology, insieme a Tristan Harris, un ex manager di Google anche lui pentito. Persino chi ha contribuito a creare queste cose ammette che sono andate troppo in là.



La buona notizia è che, una volta che sai come funziona il meccanismo, puoi difenderti. Non significa che devi smettere di usare TikTok o YouTube o Instagram: significa che puoi decidere tu quanto tempo dedicargli, invece di lasciare che sia l'app a decidere per te.



La prima cosa da fare è usare il timer. Quasi tutti gli smartphone ti permettono di impostare un limite di tempo per ogni app. Quando il tempo finisce, l'app si chiude. È fastidioso, un po' come quando la mamma dice "basta televisione", solo che stavolta sei tu a dirtelo da solo. Ma funziona, perché il momento più difficile è proprio quello in cui devi decidere di smettere, e il timer lo fa al posto tuo.

La seconda cosa è disattivare l'autoplay. Sia su TikTok che su YouTube esiste un'impostazione che impedisce al video successivo di partire da solo. Quando il video finisce, lo schermo si ferma, e per guardare il prossimo devi scegliere tu di farlo. Sembra una piccola cosa, ma ti restituisce quel mezzo secondo di pausa in cui il cervello può chiedersi "voglio davvero continuare?".

La terza cosa è togliere il telefono dalla camera da letto prima di dormire. Se il telefono è sul comodino, la tentazione di "dare un'occhiata veloce" è fortissima, e ormai sai come va a finire. Se invece è in un'altra stanza, quella tentazione non esiste. Puoi comprare una sveglia da tre euro se ti serve per svegliarti. E non è solo una questione di tentazione: diversi studi hanno dimostrato che avere il telefono in camera è collegato a un sonno più breve e più disturbato, perché le notifiche continuano ad arrivare anche di notte.



La quarta cosa è la più semplice: ogni tanto, fermati e chiediti "mi sto divertendo davvero?". Non quanti video hai guardato, non se il prossimo sarà bello, ma se in quel preciso momento ti stai divertendo o se stai semplicemente scorrendo per inerzia, come quando mangi le patatine una dopo l'altra senza avere più fame. Se la risposta è "in realtà no, sto solo scorrendo", è il momento di chiudere l'app e fare qualcos'altro. Perché alla fine non conta solo quanto tempo passi sui social, ma come li usi: guardare un tutorial che ti insegna qualcosa è molto diverso dallo scorrere video per un'ora senza nemmeno ricordarti cosa hai visto.



Camilla, quella sera, ha finito per addormentarsi con il telefono in mano. La mattina dopo alla verifica di matematica non è andata benissimo. Ma ha imparato qualcosa di importante: non era lei a decidere di guardare quei video, era l'app a decidere per lei. Da quel giorno ha messo il telefono in cucina prima di andare a dormire. Le prime sere è stato strano. Poi si è abituata. E la mattina dopo si svegliava più riposata, con la testa più libera, e con la sensazione di aver ripreso in mano qualcosa che le era scivolato via senza accorgersene.

GIOCHIAMO

CACCIA ALLE SILLABE

In ogni riga c'è una parola con una o più sillabe mancanti. Leggi la definizione, capisci che parola è, poi scrivi la/e sillaba/e mancante/i nella casella vuota. Alla fine, leggi tutte le sillabe scoperte nell'ordine delle righe: formeranno una frase segreta sulla sicurezza online!

DIPENDENZA DIGITALE E TEMPO-SCHERMO

#	SILLABA	PAROLA	DEFINIZIONE
1	---	__SERTO	Un luogo vastissimo coperto di sabbia dove piove pochissimo
2	---	LAN__A	L'arma lunga e appuntita usata dai cavalieri medievali
3	---	RIME__O	La soluzione che si trova per risolvere un problema
4	---	FOR__NA	La buona sorte, quella che tutti sperano di avere
5	-----	__TITÀ	Indica il numero o la misura di qualcosa, cioè quanto ce n'è
6	---	__PO	Il piccolo roditore grigio che ama il formaggio
7	-----	__PIO	Un antico edificio dove i Romani pregavano i loro dei
8	---	__POLO	L'insieme di tutte le persone che vivono in una nazione

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

CRITTOGRAFIA E MESSAGGI SEGRETI

#	SILLABA	PAROLA	DEFINIZIONE
1	---	__GHIA	La parte dura che cresce sulla punta delle dita delle mani e dei piedi
2	---	__RENO	Il cielo quando è limpido, azzurro e senza nuvole
3	-----	__CO	Un abitante dell'antica Atene o di Sparta
4	---	__VAGLIA	Il grande panno che si stende sulla tavola prima di mangiare
5	---	__LANGA	L'enorme massa di neve che scivola giù dalla montagna
6	-----	__BLEMA	Una situazione difficile da risolvere, come quelli di matematica
7	-----	__TO	La copertura che sta sopra la casa e la protegge dalla pioggia
8	---	__NACA	Il lungo vestito che indossano i monaci e i frati

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

🔍 RECENSIONI FALSE E TRUFFE COMMERCIALI

#	SILLABA	PAROLA	DEFINIZIONE
1	----	___NELLO	Lo strumento con le setole che si usa per dipingere
2	---	___LAME	L'insaccato di carne che si taglia a fette per il panino
3	----	___MAVERA	La stagione in cui sbocciano i fiori e le giornate si allungano
4	---	___RE	La grande distesa d'acqua salata dove si va a nuotare d'estate
5	---	GRA___NO	Ognuno dei piccoli scalini che formano una scala
6	----	___PAGNO	L'amico che si siede accanto a te in classe a scuola
7	----	___TO	La distesa verde dove cresce l'erba e si gioca a pallone
8	---	___GALO	Quello che ricevi il giorno del tuo compleanno, avvolto nella carta colorata

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

📢 PUBBLICITÀ NASCOSTA E INFLUENCER

#	SILLABA	PAROLA	DEFINIZIONE
1	----	___TOLA	Il recipiente di metallo che si mette sul fuoco per cuocere la minestra
2	---	___PONE	Quello che si usa con l'acqua per lavarsi le mani
3	----	AS___BLEA	La riunione in cui tante persone si ritrovano per discutere insieme
4	----	SOR___SA	Qualcosa di bello e inaspettato che non ti aspettavi
5	----	___TADINO	Chi lavora la terra e coltiva frutta e verdura nei campi
6	---	___VAGNA	La superficie su cui l'insegnante scrive con il gesso in classe
7	---	___LEFONO	L'apparecchio che usi per chiamare e parlare con qualcuno a distanza
8	----	___GIONE	Ognuno dei quattro periodi in cui si divide l'anno

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

PROTEGGI I NONNI DAI PERICOLI DEL WEB

1. WHATSAPP: ATTENTI AI FALSI NIPOTI

Se ricevi un messaggio da numero sconosciuto tipo "Nonna, sono io, ho cambiato numero", NON rispondere subito. Chiama tu al vecchio numero del nipote per verificare. I truffatori copiano foto profilo e nomi!

2. EMAIL SOSPETTE: MAI CLICCARE SUI LINK

Se arriva un'email dalla banca, dalla posta, dall'INPS con scritto "clicca qui urgente": NON cliccare mai! Le banche vere non mandano email con link. Cancella subito.

3. FACEBOOK: NON ACCETTARE SCONOSCIUTI

Se qualcuno che non conosci ti manda richiesta d'amicizia, anche se ha foto bella e profilo gentile: rifiuta. I truffatori creano profili falsi per studiare le tue abitudini.

4. LE VINCITE ONLINE NON ESISTONO

"Hai vinto un iPhone!", "Sei il visitatore numero 1000!": sono TUTTE truffe. Non cliccare, non compilare moduli, non dare dati personali. Chiudi la pagina.

5. SHOPPING ONLINE: SOLO SITI CONOSCIUTI

Compra solo su Amazon, eBay, siti di negozi veri che conosci. Se trovi offerte incredibili su siti mai sentiti: è truffa. Il prezzo troppo basso è sempre sospetto.

6. MAI DARE CODICI AL TELEFONO O PER MESSAGGIO

Se qualcuno (anche dicendo di essere della banca) ti chiede codici SMS, PIN, password: riattacca! Le banche NON chiamano mai per chiedere questi dati.

7. VIDEO E FOTO: OCCHIO ALLE BUFALHE

Prima di condividere video "incredibili" o notizie "shock", chiedi a noi se sono vere. Il 90% delle cose che girano su WhatsApp sono false o vecchie di anni.

8. COMPUTER LENTO? NON CHIAMARE NUMERI A CASO

Se compare un messaggio "il tuo PC è infetto, chiama questo numero": è una truffa! Chiama noi o un tecnico che conosci di persona, mai numeri trovati online.

9. DONAZIONI ONLINE: SOLO ORGANIZZAZIONI VERIFICATE

Se vuoi fare beneficenza online, usa solo siti ufficiali di associazioni conosciute (Croce Rossa, Telethon, ecc). Mai mandare soldi a privati o raccolte fondi sconosciute.

10. PAGAMENTI ONLINE: CARTA PREPAGATA O PAYPAL

Se proprio devi comprare online, usa una carta prepagata con pochi soldi sopra, mai la carta principale. Se ti truffano, perdono solo quei pochi euro.

PROTEGGI I NONNI DAI PERICOLI DEL MONDO REALE

1. LA POLIZIA NON CHIEDE MAI SOLDI

Se qualcuno telefona dicendo "Sono il maresciallo, suo nipote ha avuto un incidente, servono soldi subito": è FALSO. Riattacca e chiama tu il 112 vero.

2. NON APRIRE LA PORTA AGLI SCONOSCIUTI

Tecnici del gas, controllori, postini che non aspetti: prima guarda dallo spioncino, poi chiedi documenti attraverso la porta CHIUSA, poi chiamaci per verificare.

3. AL BANCOMAT VAI SEMPRE DA SOLO

Se qualcuno ti "aiuta" al bancomat, ti sta probabilmente spiando il PIN. Rifiuta ogni aiuto, anche se sembrano gentili. Se serve aiuto, chiama la banca.

4. NESSUNO VIENE A CASA PER RITIRARE SOLDI

INPS, Agenzia delle Entrate, Comune, Banca: NON mandano MAI persone a casa a prendere soldi, gioielli o carte. Se viene qualcuno: porta chiusa e chiama 112.

5. CONTRATTI ALLA PORTA: MAI FIRMARE

Luce, gas, telefono, assicurazioni: mai firmare nulla con persone che suonano alla porta. Anche se insistono. Di' "devo parlarne con mio figlio" e chiudi.

6. IL TRUCCO DEL "SOLDO FALSO"

Al mercato o nei negozi, se qualcuno ti fa vedere una banconota dicendo "questa è falsa, me la cambi?": è una truffa per scambiare i soldi. Rifiuta sempre.

7. FALSE BENEFICENZE PER STRADA

Persone con pettorine che chiedono donazioni per disabili, bambini, animali: molte sono truffe. Dona solo a organizzazioni che conosci, non per strada a sconosciuti.

8. ATTENZIONE ALLE DISTRAZIONI

Una persona ti chiede l'ora, un'altra "ti è caduto qualcosa": mentre sei distratto, un complice ti ruba portafoglio. In gruppo: diffidate sempre.

9. FARMACI PORTA A PORTA: SEMPRE FALSI

Nessuno può vendere medicine per strada o porta a porta. Sono sempre prodotti inutili o pericolosi. Medicine solo in farmacia, con ricetta.

10. AL TELEFONO: NESSUNA INFORMAZIONE PERSONALE

Non dire mai: se sei solo in casa, dove tieni i soldi, quali carte hai, quando torni da un viaggio. Queste cose non servono a nessuno onesto.



Glossario di Cybersecurity per Bambini

- Antivirus:** Un programma speciale che protegge il tuo computer dai virus, come un "dottore" per il computer.
- Avatar:** L'immagine o il personaggio che usi per rappresentarti online nei giochi o sui social media.
- Bug:** Un errore o un problema in un programma del computer. Come quando un giocattolo non funziona bene.
- Browser:** Il programma che usi per visitare i siti web, come Chrome, Firefox o Safari.
- Cyberbullismo:** Quando qualcuno usa internet per essere cattivo o ferire i sentimenti di un'altra persona.
- Chat:** Una conversazione online con altre persone tramite messaggi di testo.
- Crittografia:** Un modo per trasformare messaggi in codici segreti così solo le persone giuste possono leggerli.
- Download:** Quando prendi un file da internet e lo salvi sul tuo computer o tablet.
- Dati personali:** Informazioni su di te, come il tuo nome, indirizzo o età, che dovrebbero rimanere private.
- Firewall:** Un programma che funziona come un guardiano, controllando chi può entrare nel tuo computer da internet.
- Hacker:** Una persona che usa il computer per entrare nei sistemi di altre persone. Alcuni hacker sono buoni e aiutano a trovare problemi di sicurezza, altri sono cattivi.
- Internet:** La grande rete che collega computer in tutto il mondo, permettendoci di condividere informazioni.
- Link:** È un collegamento che ti porta da una pagina web a un'altra. Può essere una parola, un'immagine o un pulsante su cui puoi cliccare. Quando lo premi, vieni "trasportato" in un altro sito, documento o contenuto online.
- Password:** Una parola o un codice segreto che usi per accedere ai tuoi account, come la chiave della tua casa digitale.
- Phishing:** Un trucco in cui qualcuno finge di essere una persona o un'azienda di cui ti fidi per rubare le tue informazioni.
- Privacy:** Il diritto di mantenere le tue informazioni personali al sicuro e decidere chi può vederle.
- Social Media:** Siti web e app come Instagram o TikTok dove le persone condividono foto, video e messaggi.
- Spam:** Messaggi o email indesiderati, spesso pubblicità, che possono contenere virus o truffe.
- Virus:** Un programma dannoso che può danneggiare il tuo computer o rubare informazioni, come un "raffreddore" per il computer.
- Wi-Fi:** Il sistema che permette ai dispositivi di connettersi a internet senza fili.

Partecipa al mondo di Attentionline Junior!

Hai idee per rendere il web più sicuro per i giovani navigatori? Sei un insegnante con suggerimenti per attività in classe? O forse sei un ragazzo con domande sulla sicurezza online? La tua opinione è importante!

Scrivici a junior@attentionline.it - insieme possiamo creare un internet più sicuro e divertente per tutti!